THE UNIVERSITY OF QUEENSLAND

AUSTRALIA

High-efficiency quantum photonics

Devin Hugh Smith

B.Sc. (Eng), Queen's University at Kingston

M.Sc., University of Waterloo

May 21, 2014

A thesis submitted for the degree of Doctor of Philosophy at The University of Queensland in 2013

School of Mathematics and Physics

Abstract

This thesis examines the integration of two disparate technologies in order to perform experiments in single photon quantum optics with low loss. Many technologies and experiments in quantum optics, communication, or computing require a certain fraction of the photons involved to be received at the end of the experiment, and in many cases the required efficiency has not yet been reached. This includes the famous Einstein, Podolsky, and Rosen *gedanken-experiment*, now implemented in the laboratory, demonstrating the existence of entanglement to unconvinced observers. Also included is the nonlocality test of John Bell, as well as technological problems such as device-independent quantum key distribution. In this thesis I perform these experiments in the high-efficiency regime.

This programme requires the integration of two lines of research: improving sources of single photons, and improving detectors thereof. Until recently detector research was focussed on development, with improvements being sought for their own sake, working towards the ultimate goal of perfect photon detection. Recent years have seen these devices move into quantum photonics laboratories, allowing for previously impossible experiments to be undertaken.

In this thesis, I combine high-efficiency, number-resolving, detectors with a high-efficiency entangled photon pair source, based on another line of research going back decades: the use of spontaneous parametric down-conversion to create single-photon-like modes of light, and the entanglement of the output modes in a useful way. For small demonstrations, such as the experiments mentioned above, this can emulate a single photon with enough fidelity, and low enough loss, to successfully perform the procedure.

Here I push both of these technologies, and the problems of combining them, as far as I can, and solve the problems inherent with any marriage of disparate devices. I also examine the relative performance of two different steering inequalities, one linear and one quadratic, in the presence of noise, analysing my experimental data with each of them. I perform a detection-loophole free demonstration of EPR steering, violating the local bound by 200σ, setting a then world record for efficiency at 62.5%.

Declaration by author

This thesis is composed of my original work, and contains no material previously published or written by another person except where due reference has been made in the text. I have clearly stated the contribution by others to jointly-authored works that I have included in my thesis.

I have clearly stated the contribution of others to my thesis as a whole, including statistical assistance, survey design, data analysis, significant technical procedures, professional editorial advice, and any other original research work used or reported in my thesis. The content of my thesis is the result of work I have carried out since the commencement of my research higher degree candidature and does not include a substantial part of work that has been submitted to qualify for the award of any other degree or diploma in any university or other tertiary institution. I have clearly stated which parts of my thesis, if any, have been submitted to qualify for another award.

I acknowledge that an electronic copy of my thesis must be lodged with the University Library and, subject to the General Award Rules of The University of Queensland, immediately made available for research and study in accordance with the Copyright Act 1968.

I acknowledge that copyright of all material contained in my thesis resides with the copyright holder(s) of that material. Where appropriate I have obtained copyright permission from the copyright holder to reproduce material in this thesis.

Publications during Candidature

1. D.H. Smith, G. Gillett, M.P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H.M. Wiseman, Sae Woo Nam & A.G. White.
   Conclusive quantum steering with superconducting transition-edge sensors
   Nature Commun. **3**, 625 (2012)

2. J. Laredo, M.A. Broome , D.H. Smith & A.G. White.
   Quantum holonomic phases of higher-dimensional parameter spaces
   Physical Review Letters **112**, 143603 (2014).

3. D.H. Smith, G. Gillett, M. Ringbauer, A. Fedrizzi, M.P. de Almeida, C. Branciard, A. Lita, B. Calkins, T. Gerrits., Sae Woo Nam & A.G. White.
   Experimental one-sided device independent quantum key distribution
   In progress.

Publication included in the thesis

D.H. Smith, G. Gillett, M.P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, H.M. Wiseman, Sae Woo Nam & A.G. White. *Conclusive quantum steering with superconducting transition-edge sensors* Nature Commun. **3**, 625 (2012)
Incorporated as appendix C

Contributor	Statement of contribution
D.H. Smith	Initial concept (25%)
	Source design and development (80%)
	Experiment design and construction (70%)
	Data collection (60%)
	Data analysis (50%)
	Manuscript (20%)
	Installation of detectors (25%)
	Operation of detectors
G. Gillett	Experiment design and construction (20%)
	Data collection (40%)
	Data analysis (50%)
	Manuscript (15%)
	Electronics & computer automation
M.P. de Almeida	Manuscript (15%)
	Laboratory support and management (30%)
	Experiment design and development (10%)
	Installation of detectors (25%)
C. Branciard	Initial concept (25%)
	Theory and modelling (80%)
	Manuscript (20%)
A. Fedrizzi	Manuscript (15%)
	Source design and development (20%)

Continued on next page

Contributor	Statement of contribution
	Laboratory support and Management (40%)
T.J. Wienhold	Manuscript (20%) Laboratory support and management (30%) Installation of detectors (25%)
A. Lita	Provision of detectors (25%)
B. Calkins	Provision of detectors (25%)
T. Gerrits	Provision of detectors (25%)
H.M. Wiseman	Initial concept (25%) Theory and modelling (20%)
Sae Woo Nam	Provision of detectors (25%) Installation of detectors (25%)
A.G. White	Initial Concept (25%) Manuscript (15%) Funding and support Supervision

Contributions by others to the thesis

No contributions by others except as inclusions in the paper, except for figures 2.2, 5.1 (both courtesy C. Branciard) and 5.3 (courtesy A. Fedrizzi).

Statement of parts of the thesis submitted to qualify for the award of another degree

None.

Acknowledgements

For those that made this thesis possible, my thanks.
For those that made this thesis probable, my gratitude.
For those that made this thesis bearable, my sanity.
For those that I am far away from, I miss you. I'll come visit, someday

To the friends I made in Brisbane: Thanks for making my years here enjoyable. I'll move away, but I won't stop being me. You're all invited to visit, and I'll be back.

To my colleagues at the QT Lab: You guys are great. Keep on keepin' on, because you're doing it right.

To Andrew: Thanks for having me. You're inspirational and brilliant. I hope you get some sleep soon.

To my family goes my love. I'm not the best at phoning home, but I do think of you. You can feel free to keep reading if you want to be impressed by jargon and big words, but it's not required.

To Ania, the world. You can have me back now, the thesis is done.

Keywords

Keywords: quantum optics, quantum communication, non-locality, quantum key distribution, quantum information, entanglement, superconductivity, cryogenics

Australian and New Zealand Standard Research Classifications (ANZSRC)

ANZSRC code: 020604 Quantum Optics (60%)
ANZSRC code: 020603 Quantum Information, Computation and Communication (40%)

Fields of Research (FoR) Classification

FoR code: 0205 Optical Physics (40%)
FoR code: 0206 Quantum Physics (40%)
FoR code: 0999 Other Engineering (20 %)

Contents

List of tables

List of figures

List of Abbreviations

BBM92	A QKD protocol from [BBM92].
BBO	$\beta-$Barium borate
BiBO	Bismuth borate
CFD	Constant fraction discriminator
CH	Clauser and Horne. See [CH74]
CW	Continuous wave
EOM	Electroöptic modulator (Pockels cell)
EPR	Einstein, Podolsky, and Rosen
FC	Fibre coupler
FC-PC	Fiber coupler-parallel contact. A type of fibre optic tip.
FPGA	Field programmable gate array
H	Horizontal
HWP	Half wave plate
KTP	Potassium titanyl phosphate
LHV	Local hidden variable
LN	Lithium niobate
PBS	Polarising beam splitter
PMT	Photomultiplier tube
POVM	Positive operator-valued map. A generalised measurement.
PP	Periodically poled
QKD	Quantum Key Distribution
QWP	Quarter wave plate
RTP	Rubidium titanyl phosphate
SPAD	Single-photon avalanche diode
SPDC	Spontaneous parametric down-conversion
SQUID	Superconducting quantum interference device
SSPM	Solid state photomultiplier
TES	Transition edge sensor
UQ	University of Queensland
VLPC	Visible-light photon counter
V	Vertical
WP	Wave plate

Chapter 1

Introduction

Welcome.

This thesis is about an experimental program combining disparate elements of quantum optical research in an attempt to reach the high efficiency limit. While the results are not a scalable quantum computer, I will demonstrate some fundamental non-local results.

This thesis appears in four broad strokes. The first, chapter 2, motivates the research and lays out the reasons why the particular approaches were taken. The second, chapters 3 and 4, explains the sources and detectors of light used, as well as giving some technical guidance for a those working with these technologies in future. The last scientific section, chapter 5, reports the experimental results arising from this research effort. Finally, two technical appendices cover the hard-won technical knowledge from my degree, hopefully reducing to an undergraduate practicum problems that took months to solve.

Before I get into the nitty-gritty of photon production and detector properties, let's first take a look at some historical—and personal—context. Why is it that people are playing with single photons? Why optics instead of solid state? Why am I in Australia, working on this?

Single photonics is an 'easy' test-bed for quantum mechanics, and for technologies that build upon it: the mathematics is extremely simple[1], and approximates the real system with unparalleled accuracy. This allows tests of ideas, quantum mechanics, and technologies without complication due to 'messy' environmental interaction.

In fact, there are *no* surprising experimental results with single photons. *All* of the interesting work is actually in technical development; 'fortunately' there's plenty of it to do.[2] That technical development is what brought me to quantum optics: the dream of the quantum

[1] For a quantum system, at least

[2] Unfortunately, the technical development seems to be unpublishable. Therefore, the standard scheme seems to be to spend ages figuring out how to solve some technical problem and then do an easy experiment demonstrating it and act like the experiment was important as something other than a demonstration of your new technology. The progress of science works in mysterious ways.

computer as an engineering problem. On the face of it, the problems facing optical quantum computing are simple, but of course easily understood problems aren't necessarily easy to solve. Several scientific breakthroughs will need to occur before a quantum computer with photons as qubits will be feasible.

Quantum computing isn't, however, the most mature of the new quantum technologies that are applicable to optics: quantum communication, primarily in the form of quantum key distribution, is starting to be commercialised (for instance, [IDQ; Mag]).

In some sense, the problems of quantum communication—primarily quantum key distribution—*are* now engineering problems. The technical capability to communicate quantumly exists [BB84], the problem now is in extending the range and speed of such communications systems to useful levels. For some work on that topic, see [Nau+13; Stu+09], but note that extending the range of a system ultimately might require a so-called quantum repeater [Mun+08], a device that uses teleportation to move quantum information long distances without destroying it. Such a gadget *will* still require additional fundamental scientific advances to be made. There remain protocols to explore, and levels of paranoia to reach, and I will do so later in this thesis.

For quantum computing, however, there are fundamental advances to be made: sources of light are still very far from good enough, for instance. At the start of this candidature our laboratory was not positioned to work on these problems; at the time integration, however, was a neglected area of research in quantum optics that we are chose to develop.

Many technologies have been developed recently, more quickly than I anticipated—excellent detectors, improved sources of photons, and methods of integrating them into waveguides or other integrated optics.

What has been lacking, however, is work actually combining these elements. The problem of using, say, a high-efficiency source as a device, rather than as the object of study, turns out to be nontrivial. Ultimately, all of those elements—and more—must be combined if a quantum computer is to be made.

In our lab various projects are underway in that direction. A 'true' single photon source is being worked on, to replace our current generation of sources. Collaborations are underway to move our quantum circuits from bulk optical systems to integrated waveguides, with a first generation of such circuits under test at present, for which a thesis should appear later this year. And then there's my own study: using a set of detectors with near perfect efficiency as the endpoint of experiments.

I am not making scientific breakthroughs in this work: the only records broken are those of efficiency[3]. Instead, I am trying to bring the reality of the quantum computer closer to reality by advancing the techniques and technologies that will be used therefor.

[3] Records subsequently rebroken by others.

Chapter 2

High efficiency quantum optics

Before I can start talking about how I approached the problem of improving efficiency in quantum optical experiments some motivation of the project seems in order. Why are we interested in increasing efficiency, why did the particular techniques used in my experiments get chosen, and what else have people done?

2.1 Why high efficiency?

My personal motivation for this project comes from quantum computing. Ultimately, the goal is to build a quantum computer; to do so requires certain things to be true[1]:

1. A scalable physical system with well characterized qubits
2. The ability to initialize the state of the qubits to a simple fiducial state, such as $|000...\rangle$
3. Long relevant decoherence times, much longer than the gate operation time
4. A “universal” set of quantum gates
5. A qubit-specific measurement capability

A cursory glance at the list will show that photonics is good-to-go on items 2-4, and in fact is most of the way there on numbers 1 and 5 as well, missing only repeatability.

Here I’ll need to bring another important ingredient of scalable quantum computing in order to quantify ‘scalable’: error tolerance. Shor [Sho95] discovered that quantum computers—like traditional digital computers but *unlike* analogue ones—can tolerate some amount of error while still outputting correct results with only a reasonable slowdown in computation speed;

[1] These are the DiVincenzo criteria[DiV00] for scalable quantum computing, widely accepted as necessary but perhaps not sufficient.

the slowdown factor is polylog in the size of the problem. That is, the computation usually takes an amount of time t, after error correction it will take no longer than $t \log^n(t)$ (for some n). An interesting historical note is that the theory of classical error correction for computation was extensively developed when early computers were unreliable and people were worried that even minute errors would ruin a computation; as it turned out by the time people were performing reasonably complex computations on an electronic computer they were so reliable that the error correction was not used. However, all that theory became useful again when encoding data for storage, for transmission, and again for quantum computing.

The amount of error that can be tolerated in a quantum computation depends on what *kind* of error is occurring. For errors typical in other architectures (based on massive particles of some kind) the typical noise threshold is about 1% for the dephasing or depolarising noise typical therein. However, this kind of noise is unusual with photons, instead the typical error with photonic qubits is simple loss, which has a much more generous error threshold of 1/3 [VBR08]. Future moves to integrated quantum optics may introduce worse noise sources some as solids are more complicated media than air, and these interact poorly with photon loss for thresholds.

Let me say that again, as it's a key motivating factor for this work: if you can manage not to lose 2/3 of your photons while performing your computation you can make a scalable quantum computer.

2.1.1 Bell nonlocality

With that in hand, let's look at another category of high-efficiency experiments: those that probe the fundamentals of physics. Einstein, Podolsky and Rosen, in one of the most cited papers ever [EPR35][2], point out that, given a particular definition of 'real', that quantum observables describing non-local particles cannot all simultaneously hold definite values, despite being perfectly correlated. Ergo, one of the following must not be true:

1. The universe is non-local
2. The universe is not 'real' in the sense of the paper.
3. Quantum mechanics is incomplete

[2] 10 years ago, the EPR paper was not even in the top tier of most cited papers in the Physical Review [Red05]. However, quantum computing/information/communication papers perpetually want to motivate their discussions of entanglement and teleportation, and it's *de rigeur* to talk about EPR to do so, leading to an explosion in citations in the last 20 years (more than 90% of the citations to the paper date from 1993 or later). I, obviously, am not immune to this.

Years later, John Bell [Bel64] noticed that, in fact, quantum mechanics was instead actually incompatible with EPR's local realism—rather than merely an incomplete description thereof—and proposed an experiment to test if quantum mechanics or local realism was incorrect; the first such experiments were performed by Aspect, Grangier, Dailbard, and Roger in 1981-2 [AGR81; AGR82; ADR82].

As groundbreaking and important as those experiments were, there was a critical flaw with them insofar as disproving local realistic theories: they weren't nonlocal, as called for in the *gedankenexperiment* of EPR. It turns out to be difficult to prove things about nonlocality in a local experiment, as was rapidly pointed out by people whose philosophies were much more comfortable in a local & real universe. In order to perform an experiment whose results would be incompatible with local realism, two (major) requirements must be met:

1. The measurement events must be made *non-locally*: that is, a photon couldn't pass between them. Moreover, the choice of which measurement to make must also be nonlocal. This loophole was closed in photonics by my Master's supervisor, Gregor Weihs (with help from his research group) during his PhD [Wei+98].

2. The measurements must be fair. In particular, one cannot assume that photons lost for whatever reason were lost uniformly at random (the "fair-sampling assumption"), which assumption nearly all experiments in photonics make, including those of Aspect. If you fail to detect enough photons one cannot violate the EPR hypothesis, it turns out [Ebe93] that one must detect at least 2/3 of the photons to do so[3]. We had hoped to close this loophole in our experiments and failed to do so (see Section 5.5). Fortunately for the cause of science Giustina, Mech, Ramelow, Wittmann and others [Giu+13] published a paper earlier this year closing the loophole: Christensen and collaborators dispute that closure, and demonstrate one of their own, in [Chr+13].

At the present time, no experiment in any medium has closed both these loopholes simultaneously; I expect that there are ongoing efforts to do so at the present time and look forward to seeing those results.

2.1.2 Einstein-Podolsky-Rosen steering

However, Bell nonlocality is not the only form thereof: So-called 'EPR-steering', or quantum steering, or 'the EPR criterion'[4] is another class of non-locality, weaker than Bell's but stronger

[3] As far as I am aware the equality of this 2/3 and the one in the prior section is entirely coincidental. Many people have squinted at the two problems, trying to figure out if it is due to some other factor, but as yet no conclusions have made it onto the pages of a journal.

[4] In single photonics this is usually referred to as steering, while it as used widely in other systems as an entanglement witness as the EPR criterion in a trusted-user paradigm.

than simple entanglement. This is the class of non-locality where one party can convince another, doubting, party of the existence of entanglement. Contrast this to a Bell test where both parties can be doubtful, and an entanglement witness is only conclusive evidence of entanglement if both parties are trusted.

A steering experiment follows the *gedankenexperiment* laid out in Einstein, Podolsky, and Rosen [EPR35]:

1. A system is partitioned between two users, canonically named Alice and Bob.
2. Bob chooses a measurement to perform upon his part of the system and informs Alice thereof.
3. Alice predicts Bob's measurement outcome (without access to his part of the system).
4. Bob measures his part and compares it to Alice's prediction.

If Alice's success in predicting Bob's outcome is too frequent, and thus is incompatible with classical mechanics, Bob must be convinced of the existence of entanglement in the bipartite system. Note however that Bob must rely on his own ability to perform measurements, and on Alice's inability to interact with his state, in order to execute this protocol. The former can be satisfied by careful characterisation of his system, as I will discuss later, while the latter can be addressed in several ways. The traditional approach, following EPR, is for steps three and four, above, to be space-like separated, as in the Bell nonlocality test, while in our paper we make a more technological argument.

A primary use for steering is for a user to be convinced that he shares entanglement with another, remote, user. He cannot trust the remote user to operate their equipment carefully, nor make the correct measurements, so challenges her to steer his results. So long as the source of the quantum states is independent of the other user they can even prearrange the series of measurements that will be made.

The remote user, of course, can in their own perspective be the trusted local user and the procedure can be repeated with Alice and Bob inverted, so she challenges him to steer her results as well. If both parties can have their states steered then each can be sure they share entanglement.

On the other hand, if one of the parties is trusted, say a bank, then only one of the two must be steered to assure that the link is entangled; the quantum channel can then be used for simple quantum key distribution.

Steering inequalities, being easier to violate than Bell inequalities, have a lower efficiency threshold, and in fact a slightly different efficiency measure. Only loss at Alice's—that is the untrusted—side matter, as Bob doesn't notice when his detectors fail to fire. Thus, *Alice* must detect some fraction of events, rather than the two parties together reaching a threshold number; as it happens the tolerable loss is $(N-1)/N$ of the photons if Bob chooses from N bases to measure in. As discussed later, there is a possible security flaw for $N > 2$, so the most-important limit is loss less than 1/2.

2.1.3 Quantum key distribution

Quantum Key Distribution (QKD) is a fundamental technology in quantum communication—indeed, QKD was the first commercial product arising from the rise of quantum information. QKD allows two remote parties to generate a shared key—a secret random bit-string[5]—that can be used for a variety of purposes, the typically encryption of messages between them, and authentication of identities.

Let's first look at how the encryption process works. The most secure encryption known—indeed, the only provably secure encryption process without any assumptions—is known as the one-time pad, and works as follows:

1. The two counterparties, Alice and Bob, must pre-share their secret key.

2. Alices encodes her message digitally, say in ASCII[6].

3. Alice takes the bitwise exclusive or (XOR)[7] of her message with the secret key to generate the encoded ciphertext, which can be broadcast to Bob on a public channel.

4. Bob repeats the same procedure as Alice, taking the XOR of the secret key and the ciphertext, yielding the encoded message[8].

So long as the secret key is used exactly once this procedure is information-theoretically secure against attacks, given an uncompromised, random, secret key, as the output is another uniformly random string. Each possible message is equally likely to be encoded in a given ciphertext.

However, if the secret key is used twice, the security falls apart—the XOR of the two messages will remove the key entirely, leaving two messages to disentangle from one another. Famously, during the Cold War every message so encoded and intercepted by the other side was stored and checked against all prior messages for key reuse, with occasional success. It turns out to be difficult to get new secret keys to intelligence agents imbedded in delicate positions.

[5] *i.e.* number

[6] Any encoding will do. In fact, this works on plain english text modulo 26 just as well as on bit strings, which is how spies have traditionally used a one-time pad.

[7] This is bitwise addition modulo 2. On alphabetic text, use addition modulo 26.

[8] XOR is self-inverse. On alphabetic text, use subtraction modulo 26.

So given that there is a perfectly secure way to encode messages given a secret key the task reduces to distributing such keys to interested counterparties. The traditional way to do so is via a suitcase full of data, which has some practical limitations.

The quantum solution to the problem is to use the correlations of entangled states, given by steering and limited by the uncertainty principle, to generate the shared secret key. The scheme I am going to present here is due to Bennett, Brassard and Mermin [BBM92]:

1. Alice and Bob agree on two common orthogonal measurement bases, $i \in \{1, 2\}$.
2. A singlet state of two qubits $(|01\rangle - |10\rangle)$ is sent to Alice and Bob
3. They each independently measure their qubit in a randomly chosen basis and receive a random outcome $\{A, B\} \in \{0, 1\}$.
4. Each publicly declares their choice of basis for each measurement, and for events where they have chosen different bases or either has failed to receive a photon they discard that measurement.
5. An error-correction procedure is used to ensure that the two users have the same bit string, and a privacy-amplification procedure is used to ensure that the error correction hasn't given a third party access to part of the key[9]. So long as the bit error rate is lower than some threshold some amount secret key can be found, with the exact value depending on the protocol and model. For the base BBM92 scheme it is 14.4% [BBM92]

The scheme presented above should be compared with the procedure used for steering; the only difference is that rather than Alice being directed in her basis choice by Bob, she chooses at random and they compare their selections afterwards. This difference is because of the choice of adversary: rather than Alice convincing Bob of something, Alice & Bob are working together to defeat the eavesdropper Eve.

The BBM92 protocol works in post-selection—only when both Alice and Bob receive a photon does the event register. This leaves it vulnerable to various attacks that depend on the detection apparatus, in particular to measurements being made improperly: either because one of the counterparties is incompetent or because a third party causes the measurements to give them bad data.

However, QKD is otherwise provably secure: the *only* assumption that need be made is that the two parties' detection apparatus is secure and correct[10].

[9] These can be integrated together in some protocols.

[10] And that they don't do something obviously stupid like transmit their detection results to an eavesdropper. It turns out that most of the vulnerabilities found in QKD so far have been of this kind, with detectors that broadcast their results to an eavesdropper.

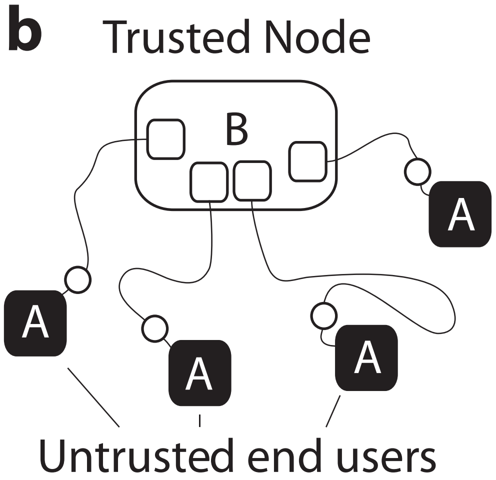

Figure 2.1: A model for the use of 1SDI-QKD: a large trusted node B, say a bank, wants to communicate with a variety of end users A who can't be trusted to successfully operate fancy quantum-mechanical equipment which is thus treated as a black box. The parties A are assumed to be acting in good faith with the party B, so they can faithfully report information they receive. The photons for this service can be provided by an independent third party or by either party, as long as the source is not inside the measurement black box.

2.1.4 Device-independent quantum key distribution

Device independent QKD gets around such limitations: it makes no assumptions as to the quality of the detection apparatus, and instead guarantees security independently of the qualities of the two measurement devices.

In the case of fully device-independent QKD, it does so via measuring a Bell parameter, with the difficulties that ensue (see section 5.5) plus an overhead due to the need for security over-and-above the proven nonlocality. It turns out that the efficiency required for such a protocol is about 91%[11], which remains outside the possible for now.

However, a colleague at UQ, Cyril Branciard, and some collaborators [Bra+12] have come up with an intermediate class of device independence: one of the two apparatus, say that of Alice, is untrusted and we are thus insured against measurement errors therein, while the other detection apparatus remains, as in BBM92, a trusted device. (See figure 2.1.)

We thus are in a position where there is one black box and one white box device, exactly analogous to the position for measuring a steering inequality. However, the efficiency threshold for QKD is higher than to simply violate a steering inequality, with efficiency $\eta > 65.9\%$ required for perfect visibility.

[11] Symmetric heralding

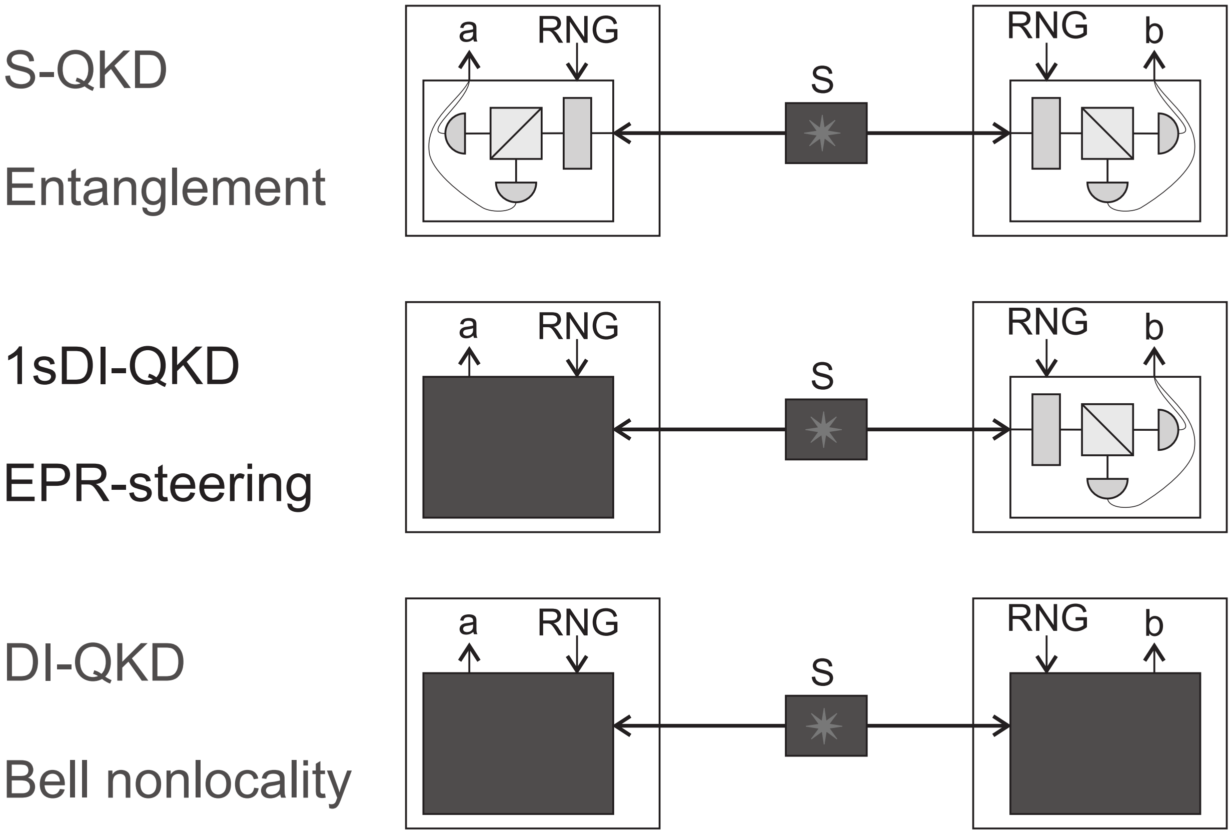

Figure 2.2: A comparison of the various classes of device-independence for quantum key distribution. Standard QKD's security is based on shared entanglement, but requires both parties' measurement apparatus to be correctly implemented. Standard QKD also never becomes vulnerable to loss. Device independent quantum key distribution, on the other hand, doesn't require either party to correctly operate their measurement apparatus to ensure security—if their measurements are incorrect, the protocol fails instead. However, such reliability places greater constraints upon the users—their security relies upon Bell nonlocality, which requires them to lose no more than 9% of the photons.
In an intermediate position, one-sided device independent QKD (1sDI-QKD) asymmetries the protocol in a manner analogous to a steering protocol—one of the parties' apparatus is trusted to be correct, while the other is treated as a black box. This relaxes the constraints on efficiency from 91% to 65.9%, which should be within our grasp using current technology, and also extends the possible range of the protocol even in theory, as some loss is always due to transmission distance.
Figure courtesy C. Branciard

Table 2.1: Losses in the experimental system during the steering experiment. Our detectors had a dead time after each photon struck them, leading to loss, the value here assumes a detection rate of about 12.5 kHz. Several values are estimated from best-known data, and the total of the known losses (about 27%) is significantly lower than the loss in the experiment of 38%, which can be attributed to misalignment. Background loss is the effective loss introduced due to stray light arriving at the detector: each of these photons is a false positive. The theoretical best-performance of the Sagnac source is listed as 'Source optimisation'.

Source	Number	Loss per (%)	(dB)	Total loss (dB)
Source optimisation	1	10	0.40	0.40
Background				0.05
Detector pileup		2.5	0.11	0.11
Detector efficiency	1	2	0.09	0.09
SM9/125–SMF-28e splice	1		0.09	0.09
SMF-28e–SMF-28e splice	2-3		0.02	0.04-0.06
Interference filter	1	4	0.34	0.34
Coated glass surfaces	8		0.02	0.16
Mirrors (dielectric)	1	1	0.04	0.04
Total		27		1.32

2.2 Why these technologies?

Given that we want to implement some high-efficiency quantum optics for quantum information processing the choice of technologies for various parts of the experiment need to be decided. In particular, the choice of photon source and photon detector is critical.

2.2.1 Medium

The first major choice, though it may not seem to be one, is the choice of free space versus integrated optics. While the majority of experiments in quantum optics so far have been performed in with free space (or 'bulk') optics, there has been much movement towards integration in the last few years.

Traditionally, quantum optics is performed with laser beams (or single photons in an approximately Gaussian beam) in free space, manipulated by bulk optical elements. This approach has several advantages: it's a well understood technology; the parts are readily available; and air is a low-loss, linear medium.

So if everyone's always used bulk optics and they have many things going for them, obviously there must be some drawbacks in order for me to include this section in this thesis, and indeed there are. The most obvious in the long term is simple and apparent upon reflection: bulk optics are bulky. The footprint of a single quantum gate made from bulk optics in our lab is about 25 cm square; to perform a meaningful quantum computation will require on the order of thousands of quantum gates, just as it does in a classical computer. At sixteen gates per square meter a fairly large laboratory would be required just to house the quantum computer. Unfortunately, that's not the end of the story—if that were the only problem I'd be happy to start big and figure out how to make it smaller later. However, those gates also require a long time to set up (about a person-week, if I'm feeling generous) and need basically constant maintenance to maintain their alignment, as well as being highly sensitive to fluctuations in temperature, due most probably to thermal expansion and contraction of focussing elements. In principle, the alignment could be automated by replacing manual with computer-driven actuators, but to my knowledge no one has yet demonstrated self-aligning quantum optical processes.

The other problem with bulk optics which may not be apparent is that of integration. While a network of quantum gates made of beamsplitters and waveplates[Rec+94] can probably be created *en bloc*, the sources and detectors of light are more complicated. It seems unlikely that true single photon sources will be made in bulk(*q.i.*), so you have to couple that light to your bulk network somehow. Even for current sources, like the ones I used, the light is often coupled to fibre optic to constrain it to useful modes.

As most good detectors are cryogenic, they require the incoming light to be confined to a fibre before the detector for geometric reasons. Even those detectors that are not cryocooled are much noisier if they aren't coupled to a fibre to constrain the incoming light to only the modes of interest—otherwise stray light from the experiment, or worse yet ambient lighting, can interfere with experimental operation. Therefore we usually require coupling to fibre optic, which is a lossy process that asks we let the light into free space in the first place. Note, however, that there is a significant technological gap between detectors that require fibre-coupled light and those that are actually integrated into a monolithic device.

Contrariwise, integrated optics, that is, light being confined in a waveguide of some sort while interacting with the other photons have a ways to go for single-item performance: the sources aren't as good[Eis+11], the gates aren't as good[PMO09], and the detectors aren't as good[Ger+11]. Worse yet, consensus on what kind of integrated optics are optimal hasn't yet been reached. Current technologies being explored somewhere include silica-on-silicon, silicon, silicon carbide and gallium arsenide lithographic waveguides, and silica laser-written or fibre-based waveguides. Some of these technologies are in use in the telecommunications industry for moving classical information around (*i.e.* the internet), while others are almost entirely research material.

The draw of integrated optics is repeatability and size: if you can design one of something and have it come out of fabrication, you can (in principle) have as many more as necessary; as the total size of the components is measured in cubic millimetres instead of decimetres the whole computer is much smaller. Moreover, if you have designed your source, gates, and detectors to all be integrable there should be no problems interconnecting the pieces.

Unfortunately, repeatability doesn't get you anywhere if you don't have anything worth repeating, which is currently the state of play in integrated optics for quantum information. At the time of deciding how to proceed with parts of this project[12] no integrated detectors had been demonstrated, and the best integrated sources were both noisy and inefficient; [Eis+11] given that good detectors were on hand for a bulk experiment the obvious decision was to work with the best available bulk sources and processes, and leave developing good integrated sources and detectors to other projects.

Let's examine the two critical pieces, sources and detectors, next.

2.2.2 Sources

It turns out that the biggest outstanding problem for quantum information using photons is simply (and somewhat embarrassingly) making single photons. If one takes a traditional light source—an incandescent lightbulb, a laser, a flame—and attenuates it, the discovery is quickly made that the emission from such a device does not have definite photon number.

The most useful of these for quantum experiments is the laser, which outputs coherent states of light. In a reasonable sense coherent states are the 'most classical' states of light, so it's vaguely surprising that they come from lasers, which fundamentally rely on quantum mechanics to operate. Of course, laser beams are not perfectly coherent, but that minor detail is irrelevant here. The coherent state $|\alpha\rangle$ is

$$|\alpha\rangle = \exp\left(-\frac{|\alpha|}{2}\right)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{2.1}$$

in the photon number basis, where α is any complex number and $|n\rangle$ is the state with *exactly* n photons in it.

It doesn't take a lot of figuring to figure out that the coherent state doesn't very closely approximate the single photon. No matter what α is chosen, two things are true: you cannot get a single photon more than

$$\frac{1}{e} < \frac{2}{3}$$

of the time, and yet that's not even the worst of your problems.

There are two worse problems: first, you can't tell when you do have your single photon. In principle, a magical non-demolition measurement of photon number can solve this problem. In

[12] Some years before I was involved, in the case of the transition edge sensors

practice I would be astonished if such a thing ever eventuated for free-flying optical photons[13]. Secondly, and less obviously, you make *more than one photon* a fair fraction of the time. While this doesn't seem like a problematic failure mode at first glance, it turns out that accidentally making too many photons is a much bigger problem than losing some. Given that we are losing some photons, additional loss at the source isn't so bad. We just want to avoid accidentally having the expected number of photons, since then we get a false positive; that is, if we make zero photons in mode A and two photons in mode B there's a fair chance that all seems well but we get a logical error somewhere in our computation. Whilst cleverness in circuit design can mask this problem somewhat it cannot solve it entirely, leading to a worse error threshold. Therefore, in practice fact one must further reduce the likelihood of single photon emission by reducing the average photon number well below one.

So, given that the easy way out doesn't work, what approaches are left? As I see it, they are twofold: one can either generate correlated light via nonlinear optics, or generate 'true' single photons from a single emitter of some sort. Let's look at the second of these options first.

A true single photon source is some kind of object that can literally only emit one photon at a time: the archetypical example is a single atom. A single atom, unfortunately, is awkward to work with: keeping it in one places requires optical trapping or, if ionised, electromagnetic trapping, and problematically the emission is into $4\pi\,\mathrm{sr}$. One can enhance emission into a preferred direction by placing the atom in an optical cavity, but then the time-bandwidth product of the photon may be adversely affected due to the photon rattling around in the cavity. Naïvely, the hold time simply extends the time uncertainty of the photon, making things untenable, but the cavity feeds back on the emitter and narrows the output. It is in principle possible to make transform-limited photons in a cavity, but is definitely more difficult engineering challenge than in free space due to the additional degrees of freedom. As transform-limited photons are ideal for quantum information this degradation is a major problem.

Other true single photon sources do exist, and in fact are improving at a rapid pace. Of note are various kinds of quantum dots. Self-assembled quantum dots on a flat substrate are a popular test bed [San+01; Shi07] , but suffer from the same thing that makes them easy to work with: the self-assembly process is random, so finding a suitable dot or dots is complicated, and localising the emission into a small solid angle is nigh impossible.

Semiconductor dots deliberately fabricated (in several ways) are more promising due to the flexibility involved. Indeed, our laboratory currently has a project underway examining dots lithographically embedded in micropillar cavities [Gaz+13], which have the highest emission probability of any dot-based technology, about 80% per pulse [Dou+10]. Work is ongoing to

[13] For photons trapped in a cavity, on the other hand, this is already a reality[Say+11]. My advisor thinks I am too pessimistic.

multiplex such a source for use in quantum computing.

Dots are also appealing for the simple reason that they are made in semiconductors: if the ultimate quantum computer technology is based on integrated optics a dot-based source should be relative easy to integrate into a monolithic source-gate-detector package; this upside is of course irrelevant for the current project.

At the time we started this project, quantum dot-based sources were not particularly efficient, and in fact our lab had never used one, so while we wait with bated breath for improvements therein we were not in a position to use them for my experimental work.

The other dominant sources of single photons are in fact not generators of single photons at all: non-linear-optics based sources of correlated photons [HM86; Kwi+95]. In such a source a bright pump beam is shone through a nonlinear medium—one that doesn't have the polarisibility $\vec{P}$ linearly proportional to the electric field $\vec{E}$. Depending on the details, one can arrange that in such a medium either one or two pump photons are occasionally converted into the emission of a 'photon pair' in two possibly-distinct modes.

This approach, of course, has major problems of its own. The obvious problem—that this is a random process—is nonetheless a major one. The state generated is not a number state, nor one upper bounded by one photon per mode, so generating such a state with high probability per time bin runs into the same problem as the attenuated laser pulse mentioned earlier.

However, one can in principle solve this problem: if you have access to good detectors and a fast switching network you can detect one photon in one of the two output modes and then switch the output of the other mode into your computation; with sufficient sources of light this can generate a photon in the desired mode with high probability. Unfortunately, it's quite difficult do build such a fast switching network [JBW11], especially as detector electronics are usually quite slow in comparison to light speed, creating the additional problem of storing the putative light while deciding if it's there. This is not infeasible, and in fact the group of Paul Kwiat, amongst others, are working on it [JPK04][14].

I will instead just focus on generating two photons, which reduces significantly the difficulty of the problem. When pumping a spontaneous pair source with a continuous wave laser double pair emission is very rare, so we can treat any detection events as arising from a joint Fock state

$$a^\dagger(\omega_p - \Delta\omega) b^\dagger(\omega_p + \Delta\omega)|0\rangle \tag{2.2}$$

where $a^\dagger$ and $b^\dagger$ are the creation operators for the two output modes, ω_p is the pump frequency, and $\Delta\omega$ is the frequency splitting of the two photons[15]. If we are willing to limit our experiments to two photons, this will do the trick.

[14] That said 'not infeasible' doesn't mean 'easy'.

[15] Here I'm neglecting details of the spatial modes a and b

So, we resolve to make two photons via a nonlinear process to do some two-photon high-efficiency experiments. A spectrum of choices still remains. We want to ensure

1. That we detect the photon in mode a with high probability whenever we detect a photon in mode b,
2. That we detect the photon in mode b with high probability whenever we detect a photon in mode a (though this isn't required for some experiments),
3. As a corollary to the previous, we want to ensure that as many photons as possible in modes a and b are useful signal photons and
4. A minimum of photons in our experimental modes are noise from any source.

In general, there are two types of nonlinear media used for making photon pairs, so-called $\chi^{(2)}$ and $\chi^{(3)}$ media. In both cases, some input photons are converted into the desired output photons while conserving energy and momentum. $\chi^{(2)}$ interactions involve three photons, in this case one pump photon splitting into two daughter photons at a rate dependent on the value of $\chi^{(2)}$, which is a material property. $\chi^{(3)}$ interactions involve four photons, which complicates things slightly, as the extra degree of freedom allows for more interactions. Typically, the two input photons both come from the same mode, and the daughter photons are non-degenerate in frequency to allow them to be split from the pump; but (again typically) other processes are also supported that add significant noise to the system. $\chi^{(3)}$ processes for photon pair production are also typically weaker[16] than $\chi^{(2)}$ processes, and only usefully appear in materials where $\chi^{(2)} = 0$. Fortunately or unfortunately, that class of materials includes all materials with inversion symmetry, that is, many crystals, including all single-species crystals, and all glasses. Thus, if one wishes to make a photon pair source in fibre, silica, silicon, or other common media for waveguides one must use a four-photon interaction to do so.

However, in the bulk it is much simpler, and more efficient, to use a $\chi^{(2)}$ crystal. The choice of crystal depends on a few things: the geometry of the source, desired ease of alignment, pump power and continuity[17] and desired brightness of the source. For traditional source geometries, based on overlapping the emission of two oppositely polarised paths, various borates are in common use. The two most prominent are beta barium borate [Kwi+95] (BBO[18]), the most common crystal in use in such sources, while bismuth borate (BiBO) has a higher $\chi^{(2)}$, leading to a higher source brightness [Mat+09], but is more complicated to use due to having a less symmetric crystal structure.

[16] In reasonable configurations for the source, given that I'm comparing apples and oranges here.

[17] Pulsed lasers, especially ultrafast ones, can damage some crystals with their high-intensity pulses [F+94].

[18] The optical abbreviations for crystals have only a passing resemblance to the chemistry involved. I had to look up which 'B' element this was when writing this section, as there are several to choose from.

On the other hand, if the chosen source geometry demands it, one can emit the two photons collinearly by cheating a bit. Periodically poled crystals allow for a technique known as 'quasi-phase-matching'[19], wherein the crystal is inverted periodically, remembering that a $\chi^{(2)}$ medium doesn't have inversion symmetry. This allowis the crystal to absorb some of the momentum in the conversion process. In particular,

$$\vec{k_s} + \vec{k_i} + \frac{1}{\vec{G}} = \vec{k_p},$$

where $\vec{k}$ is the photonic momentum vector for each of the (p, s & i) pump and daughter (signal and idler) photons and $\vec{G}$ is the poling period of the crystal, or more precisely, any lattice vector of it. Since we can choose $\vec{G}$ we can engineer a crystal to allow for our preferred transition wavelengths and directions [Bra+09].

Two periodic-poled crystals dominate in usage for photon sources: periodically poled lithium niobate (PPLN[20]) [Tan+01]is used extensively for most nonlinear optical processes, as it has the highest $\chi^{(2)}$ value of any useful nonlinear optical crystal[21], but has the downside in quantum optics of producing both daughter photons in the same polarisation mode. This significantly complicates the task of separating the two photons in a collinear geometry. Separation can be done if the daughter photons are not frequency degenerate, but that implies a three-frequency system and not a two-frequency one, requiring more custom optics; furthermore dichroic mirrors generally have worse performance than polarising beam splitters.

The crystal of choice for high-performance sources is periodically poled potassium titanyl phosphate (PPKTP), which is the strongest available crystal whose output is in orthogonal polarisations [KFW06; Kuk+04]. PPKTP has two downsides which a prospective user should be aware of: first, the widely available Sellmeier equations for the index of refraction as a function of wavelength are somewhat inaccurate for typical pump wavelengths ($\approx 400\,\mathrm{nm}$); and second the crystal has a low damage threshold. This is not a problem for sources pumped with continuous-wave lasers, but rapidly becomes a problem when pumped with pulsed sources [Smi09].

Intertwined with the decision of what nonlinear medium to use is the decision of what geometry the source should have. Fortunately for the length of this thesis, this decision is actually really easy: Sagnac-type sources are head-and-shoulders above all other options for generating entangled photon pairs. A Sagnac interferometer is simply a loop about which an optical beam travels in both directions; the nonlinear crystal is placed in this ring and the emission split by polarisation on output. As the direction of travel of the light cannot be

[19] It would be helpful if things were named helpfully. No one seems to agree on how many hyphens or spaces should be in that phrase, since it's actually about phase quasi-matching. History defeats utility, unfortunately.

[20] Pronounced 'pip-lin'.

[21] At least in the visible and nearby regions.

determined *a priori* the two outputs are entangled.

This geometry was developed by Kim, Fiorentino and Wong [KFW06] as the culmination of a series of down-conversion sources. As the interferometric paths are common (due to being a loop) the device is interferometrically stable, and as the nonlinear crystal's output is collinear with the pump beam the length of the crystal can be much greater, increasing brightness. A detailed introduction to such sources appears in chapter 3, while a how-to guide to build your own appears in appendix A.

2.2.3 Detectors

A single optical photon has an energy of about 200 zJ, so most—but not all, as we shall see—conventional measurement techniques for light do not extend to the single photon regime. At some point in the measurement process the small amount of energy present in the single photon must be amplified to macroscopic levels in order to record that detection.

The first such device, no longer in much use in the context of quantum information, is the photomultiplier tube (PMT). Invented in the 1930s, a PMT is a vacuum tube[22] that exploits the photoelectric effect—the emission of electrons from a metal when struck with a photon—and multiple stages of amplification using secondary emission—the emission of several low-energy electrons from a metal struck with a high-energy electron—to generate more than sufficient gain to detect single photon events. Well-made PMTs have very low noise, and are sensitive in a wide angle, making them still very useful for experiments in particle physics and elsewhere. However, their (quantum) efficiency is limited by the photoelectric efficiency of the first stage: if the photon's absorption doesn't result in an electron emission (that is subsequently captured), the photon is missed. The optimal quantum efficiency is about 30% at UV wavelengths[Ham], so while PMTs featured prominently in early quantum optical experiments, nowadays they have been sidelined by other cheaper and/or better alternatives for our purposes.

The workhorse photon detector of most quantum optical laboratories at present is the single photon avalanche diode (SPAD)[23]. A SPAD is a semiconductor diode reverse biased above the breakdown voltage. SPADs are made of silicon for visible or near-infrared wavelengths or indium gallium arsenide (InGaAs) for telecommunications wavelengths. When struck with a single photon (with energy above the bandgap) an electron-hole pair is created, which combined with the high potential difference is sufficient to cause the diode to break down, leading to an avalanche of current that is macroscopically detectable. Feedback switches off the bias voltage,

[22] I wonder if this is a term I have to explain yet, and if not how many more years it will be before one should. A vacuum tube is a glass tube with some electronics in it and, not surprisingly, no air. The first generation of commercial electronics used these things everywhere; nowadays one can only find them in high-end audio amplifiers and laboratories.

[23] These are often called 'Avalanche photodiodes' or 'APDs' in the literature, but that term also refers to a different class of photodetector with linear response to input signals.

Table 2.2: Characteristics of several classes of detectors, including the widely used SPADs for both visible (Si) and IR (InGaAs), fast-but-inefficient superconducting single photon detectors, and transition edge sensors

Type	Wavelength (nm)	Efficiency	Rep. Rate	Dark Counts	Source
Si SPAD	600-900	0.50	5 MHz	5 Hz	[Kim+09]
InGaAs SPAD	1100-1800	0.20	75 kHz	10 kHz	[Pri]
SSPD (2009)	200-1700	0.05	1 GHz	300 Hz	[Mik+08]
SSPD (2012)	200-1700	0.95	1 GHz	300 Hz	[Ger+12]
TES	200-1700	>0.95	50 kHz	0	[LMN08]

quenching the avalanche and allowing the semiconductor to recover to the ready condition. If the diode doesn't quench fast enough then as the voltage is reapplied a secondary avalanche occurs, a condition known as afterpulsing. Tuning the diode to minimise dead time between detections while also minimising after pulsing is an important piece of SPAD design. Silicon SPADs are commercially available from several sources at a reasonable cost, making them a common device in quantum optics labs around the world and eminently useable for various proof-of- experiments. Unfortunately for the cause of quantum information, however, they ultimately are not sufficiently efficient nor free from noise for scalability (see table 2.2).

A third alternative is the visible-light photon counter (VLPC)[24]. In a slightly different form, these are called 'solid state photomultipliers', a much more useful name. A VLPC (or SSPM) consists of a layer of intrinsic semiconductor as the photon absorber, which generates an electron-hole pair. However, unlike in a a SPAD only one of the two particles participates in avalanching, typically the hole, which drifts into a highly P-doped region (with arsenic) and instigates an avalanche as the impurity band electrons are very close to the conduction band. The total avalanche gain is limited by the presence of the slowly-moving positive charges, which allows for photon counting.

VLPCs have 80% (or so) quantum efficiency in the visible wavelengths, and their close cousin the SSPM has excellent efficiency from 2-20 μm, but the response is poor in the telecom band. VLPCs were the first really exciting development in photon counting, even given their somewhat awkward operating temperature of 6-10 K. However, they are hard to get ahold of outside of the USA[25], and are also extremely expensive. By the time our lab could have bought some of these more efficient options were on the market.

A fourth alternative is the superconducting nanowire single photon detector (SSPD[26]). This

[24] Does this take the cake for 'least useful descriptive name'? While it describes what they do, this name gives absolutely no indication as to how, which the author feels is a useful part of names for things. (I am also opposed to 'the Name Effect' for the same reason.)

[25] Export controls due to their utility for military purposes constrains the purchase of VLPCs/SSPMs.

[26] Apparently the people that invented these didn't think anyone would come up with a different way to detect light with a superconductor, and they're thus known in some of the literature as 'superconducting single photon

is a meander of some superconductor designed that the heat absorbed from a single photon is sufficient to cause a 'hot spot' of the wire to become a normal conductor instead. The wire has current flowing though it in it's superconducting state such that this hot spot increases the current density through the rest of the wire above the critical current, generating our all-important output signal, and then as the hot-spot cools returning quickly to their superconducting state. Because these devices are held at cryogenic temperatures dark counts are rare compared to the semiconductor devices discussed earlier.

However, at the time this lab decided to go with another technology, SSPDs were still very inefficient—efficiencies of about 3% were the best that had been reported[Mik+08]. Due to interest from various parties the designs have improved by leaps and bounds over the past few years, with SSPD efficiencies in excess of 95% reported at conferences last year. It may be the case that future work along the lines of mine may wish to use SSPDs, but at the time they were not only not readily available they were nowhere near efficient enough. They have the strong advantage of being much faster than other alternatives, easily outputting 10^9 detection events per second, making them very useful for quantum communication as well, perhaps, as future work in quantum computing.

The first near-unit efficiency detector, though, was the transition edge sensor (TES). Larger transition-edge bolometers are used as the standard for optical power meters, and the photon counting TES is simply a scaled down version of the same device. A TES is a thin film of superconductor—I am aware of titanium and tungsten devices, along with bimetallic designs for various applications—kept below the superconducting transition temperature. The device is then biased above the critical current, slightly driving the device normal[27], and if biased correctly undergoes a (relatively) large change in resistance when struck with a single photon due to the heat so absorbed.

The second key ingredient to using these devices is amplification of that still rather small signal into a macroscopically useful one. The TES is kept in series with a small inductor that is inductively coupled to an array of superconducting quantum interference devices (SQUID[28]); a SQUID is a loop of superconductor interrupted (in this case twice) by a gap of insulator, and acts like a Mach-Zehnder interferometer for electrons with the phase set by the magnetic field through the loop. If you set up your SQUIDs and the inductive coupling thereto correctly you can get a large degree of amplification without introducing much noise to your signal.

The only theoretical upper bound on the detection efficiency of TES is the trivial one—since the process in the device itself is linear, there is no chance that once the photon is absorbed

detectors'. They're also known as 'meander' detectors, due to the word 'nanowire' meaning different things to different people.

[27] Apparently early devices had issues with runaway feedback heating the device due to being current biased; devices are now biased by a current source with a resistor in parallel to the TES to prevent this (more later).

[28] Didn't someone feel clever when they came up with that one, eh?

a signal is not output and vice versa. The only problem is then insuring that the photon actually gets absorbed into the thin film, and that problem was effectively solved some years ago[LMN08]; subsequent developments have largely been in the realm of increasing the speed and ease of use of the devices.

Thus, for our high-efficiency explorations of single photon quantum information the choice was made to use TES for our detectors. A more detailed discussion of the design and use of TES appears in chapter 4.

Chapter 3

Sagnac interferometers for photon pair production

Spontaneous parametric downconversion—a $\chi^{(2)}$ nonlinear optical process—has long been a workhorse of single-photon quantum optics, as the two output squeezed vacua emulate single photons with reasonable accuracy. However, actually utilising the output beams, and ensuring that they are entangled if that is desired, has been an active area of research.

A major step forward came with the introduction of periodically poled crystals for down--conversion. This allows the phase-matching condition to be relaxed, eliminating spatial walk-off and allowing for collinear output of the two output photons, which as a corollary makes longer crystals useful, increasing sources' brightness significantly.

The research group of Franco Wong worked on the problem of how best to set up a collinear down-conversion source, and the optimal geometry discovered thus far is to place the down-conversion crystal in the loop of a polarisation Sagnac interferometer. A Sagnac interferometer, introduced by Georges Sagnac a century ago [Sag13], consists of a loop about which a beam propagates in both directions, which can be used as an absolute measure of angular velocity normal to the loop. The first Sagnac interferometer so used—by Michelson of all people—determined the absolute rotation speed of the Earth with a loop 17 km on a side [MG25]; the complexity of the experiment was largely due to the inability to stop the Earth to take baseline measurements. In the present day the major application of Sagnac interferometers is in laser gyroscopes, which are simply Sagnac loops with a lasing medium inserted. The laser gyro is used in commercial applications as varied as the compasses in all commercial aircraft and children's toys.

A polarisation Sagnac interferometer replaces the beamsplitter used as the input and output port of the interferometer with a polarising beamsplitter, making the direction of propagation correlated with the polarisation. This, in the absence of later erasing the which-path information, makes the device an interferometer in name only. Fortunately the down-conversion process, as set up here, does erase that which-path information.

Theoretically there is a challenge in deciding the optimal focussing conditions for a down--conversion source. Several contradictory reports in the literature each consider slightly different cases, which may or may not apply in this case(The most relevant being [LT05; Mit09; Ben10]). I have generally followed Bennink's [Ben10] analysis in my apparatus, though an experimental exploration of parameters was also performed.

Practically there is a major challenge that is not present theoretically. Setting $x = y = z = \theta = \phi = 0$ for each coupler and interferometric path is trivial on paper, but turns out to be a major challenge in laboratory conditions. Some methods for optimising each of the entirely-too-many degrees of freedom will be presented later in this chapter.

3.1 Spontaneous parametric down-conversion

I am no expert on the theoretical intricacies of parametric downconversion, so this section will be a practical discussion thereof, focusing on the case collinear type-II quasi-phase-matched spontaneous parametric down-conversion. For a more detailed look, the lecture notes of Marek Żukowski [Żuk02] are a good introduction.

Parametric down conversion is a nonlinear optical process in which one photon—the 'pump' photon—splits into two—the 'signal' and 'idler'[1] photons—conserving energy and momentum:

$$\vec{k_i} + \vec{k_s} = \vec{k_p} \text{ and } \tag{3.1}$$

$$\omega_i + \omega_s = \omega_p \tag{3.2}$$

where $\vec{k}$ is the momentum vector, ω the frequency, and the subscripts p, s and i refer to the pump, signal, and idler photons respectively.

The likelihood of a single photon splitting into two spontaneously (like all other three-photon interactions) is governed by the $\chi^{(2)}$ tensor, the second-order nonlinear susceptibility tensor. $\chi^{(2)}$ is a material property of the medium through which the light passes and the relevant reduced value depends the direction of the various propagation and polarisation vectors.. Note that for all media with inversion symmetry $\chi^{(2)}$ is identically zero due to symmetry, so all three-photon nonlinear processes occur in crystalline materials. While most crystals *also* have inversion symmetry, particularly if they are single-species, all disordered media do. This leaves only the small set of crystals without inversion symmetry to have $\chi^{(2)} \neq 0$, most of which are

[1] The names are historical, and come from other three-photon nonlinear processes with one useful output in the signal mode, while the idler mode is just along for the ride. The first such case was in the radio long before people were worried about generating single photons.

quite complicated. It also turns out that to have good phase matching birefringence is helpful, ruling out another class of materials. Gallium arsenide, for instance, has a very high value of $\chi^{(2)}$ but doesn't support any phase-matched solutions.

After some mathematics[Ben10; Żuk02], the following quantum state is found to be output from the spontaneous parametric down-conversion of a single pair ($a^\dagger_{\omega_s} a^\dagger_{\omega_i}$):

$$|\Psi_{\text{SPDC}}\rangle = -i \iint_0^\infty \psi(\omega_s, \omega_i) a^\dagger_{\omega_s} a^\dagger_{\omega_s} |0\rangle \, \mathrm{d}\omega_s \, \mathrm{d}\omega_i \, . \tag{3.3}$$

Here $a^\dagger_\omega$ is the creation operator in a Gaussian mode with frequency ω, $|0\rangle$ is the vacuum state, and

$$\psi(\omega_s, \omega_i) = \sqrt{\frac{hN_p}{\varepsilon_0 \lambda_p \lambda_s \lambda_i}} s(\omega_p) \mathcal{O}(\omega_s, \omega_i), \tag{3.4}$$

is the SPDC amplitude, where ε_0 is the vacuum permittivity, $\lambda_{\{s,i,p\}} = 2\pi c / \omega_{\{s,i,p\}}$ is the free space wavelength of the signal, idler, and pump beams (where, of course, $\omega_p = \omega_s + \omega_i$), $s(\omega_p)$ is the spectral amplitude of the pump (with $\int |s(\omega)|^2 \, \mathrm{d}\omega = 1$), and N_p is the mean photon number of the pump.

Just in case those are not enough layers of recursive definitions,

$$\mathcal{O}(\omega_s, \omega_i) = \int_{\text{crystal}} \chi^{(2)}(\vec{r}) : \vec{E}_{\omega_p}(\vec{r}) \vec{E}^*_{\omega_s}(\vec{r}) \vec{E}^*_{\omega_i}(\vec{r}) \, \mathrm{d}^3\vec{r} \tag{3.5}$$

is the phase matching function, given by the spatial overlap of the electric fields $\vec{E}$ of the three modes in the crystal and the nonlinearity tensor. The three spatial modes can be of arbitrary form, but given that we are inputting and extracting light via single mode fibre optics treating them as a trio of collinear linearly polarised Gaussian modes with common waist location is helpful if difficult: earlier and easier analyses treated them as plane waves instead. Here : is the scalar product of the tensors $\chi^{(2)}$ and $\vec{E}_{\omega_p}(\vec{r}) \vec{E}^*_{\omega_s}(\vec{r}) \vec{E}^*_{\omega_i}(\vec{r})$.

Our goal is to perform high-efficiency experiments with our source, so we have to optimise the likelihood that a photon is in both of our output fibre couplers at the same time.

3.2 Entangling SPDC

The outputs of a parametric down-converter are not—in the sense that experiments usually call for—usefully entangled. Note that from here on, I'm going to treat the outputs of a down-converter as two single photons, rather than a more complete mode picture. For a two-photon experiment this is true enough, as the zero photon term does not contribute, and the higher-order terms can be treated as noise; the various photon-number terms don't meaningfully interact. Depending on the exact geometry and pumping conditions, those output photons may be entangled in the frequency and time bases; while using this entanglement to perform interesting experiments is now an active area of research, it otherwise is an impediment to creating other types of entanglement. This energy-time entanglement does also incidentally affect some two-photon interference experiments in a results-improving way [Ou07] that may mislead experimenters into thinking their experiment is better than expected.

The entanglement that is interesting technologically, however, is that of degrees of freedom that can be manipulated easily for experimental purposes, and this must be added deliberately to the state. There are, at least in the context of quantum computing, three degrees of freedom mostly commonly entangled: time, path, and polarisation.

Path entanglement is simple, in some sense: the photon is either here, or there, or in a superposition thereof; moreover, the location is entangled with the position of another photon. Unfortunately the expositive simplicity contrasts with the practical complexity: each of the paths must be interferometrically stable. In bulk optics this is a huge challenge, and in fact is typically only done with two-level entanglement and only for brief periods of the experiment. In integrated optics, however, this is likely to be the go-to method of entanglement due to the much greater degree of stability in a solid device.

Time (or time-bin) entanglement is analogous to path entanglement, but in time: the photon is either now or later. Time-bin entanglement is technically easier to implement than path entanglement, as the paths of the two photons are common (except for the delay lines necessary to create and measure the light), reducing stability concerns. This is only true if the source is pumped with a pulsed laser, giving temporal resolution to the two output times; for a CW pumped source time-bin entanglement is obtainable only by post-selection[Hal+07].

This leaves polarisation entanglement, by far the most common type of photonic entanglement in experiments. If we can design a source to emit photons into two modes with unknowable but correlated polarisation we can make a polarisation-entangled pair. Changing the basis of measurement is as simple as passing the photons through a waveplate, as opposed to needing an interferometer for the prior two types of measurement, and thus there is no need for interferometric stability of the various components with respect to each other.

For many years the method for generating the ‘unknowable polarisation’ was to consider distinct spatial modes that could contain either the signal photon (in one polarisation) or the idler photon (of orthogonal polarisation); these are so-called ‘cone’ sources[Kwi+95], and are still in use for pulsed photon generation, as the bulk crystals in use in such sources are less prone to damage than the periodically poled ones used for collinear sources[2]. However, there

[2] Periodic poling allows for the collinear geometry, which otherwise can only occur for a very limited set of wavelengths; in a periodically poled crystal the direction of propagation can be along one of the crystal’s preferred axes.

are problems with such sources that upper bounds the performance:

1. Because the direction of interest is not a preferred direction of emission the output coupler cannot efficiently select out the modes of interest, and couples some of the other photons as well, upper bounding the heralding efficiency (see section 3.4.1, below);

2. As all the photons of one polarisation (say, horizontal) have the same spectrum (say, that of the signal photon), the spectrum of each photon then providing side information as to the polarisation, limiting the ultimate performance of the source;

3. Finally 'transverse walk-off' limits performance, where 'walk-off' is defined as the property that the wave vector, $\vec{k}$, and the Poynting vector, $\vec{S} = \vec{E} \times \vec{B}/\mu_0$ are not parallel in a birefringent medium, causing the collection of photons emitted in parallel to not all be collinear.

The advantage of a collinear setup is the mitigation of exactly the problems highlighted above: the preferred direction of emission is along the axis, there is no longitudinal walk-off, and, if done correctly, the signal and idler photons are each emitted into a separate mode, but with the polarisations confounded. Franco Wong's group developed the collinear downconversion source, trying several interferometric geometries [SW00; Fio+04; Kuk+04] to optimise emission and stability, and ultimately discovered that the polarisation Sagnac interferometer was better [KFW06], and moreover simpler, than their earlier geometries.

3.3 Sagnac Sources

For a detailed guide to building your own Saganc source, please see Appendix A. There you will find a detailed technical guide to the process, which will hopefully make your task akin to an undergraduate laboratory rather than a PhD project.

Here in the main text, I'll just review the scientific plan of a Sagnac source. Please refer to figure 3.1 for a diagram of the apparatus, or figure 3.2 for a photograph thereof.

A Sagnac interferometer is a loop about which light is sent in both directions. Typically in bulk optics the light is put into the loop using a beamsplitter, and the light then bounces off a few mirrors before being recombined on the beamsplitter. At all points inside the loop the two beams are anticollinear.

Absent any other behaviour, the only phase around this loop is due to the phases of the insertion beamsplitter and due to the angular velocity ω of the loop, *i.e.*

$$\phi \propto A \cdot \omega,$$

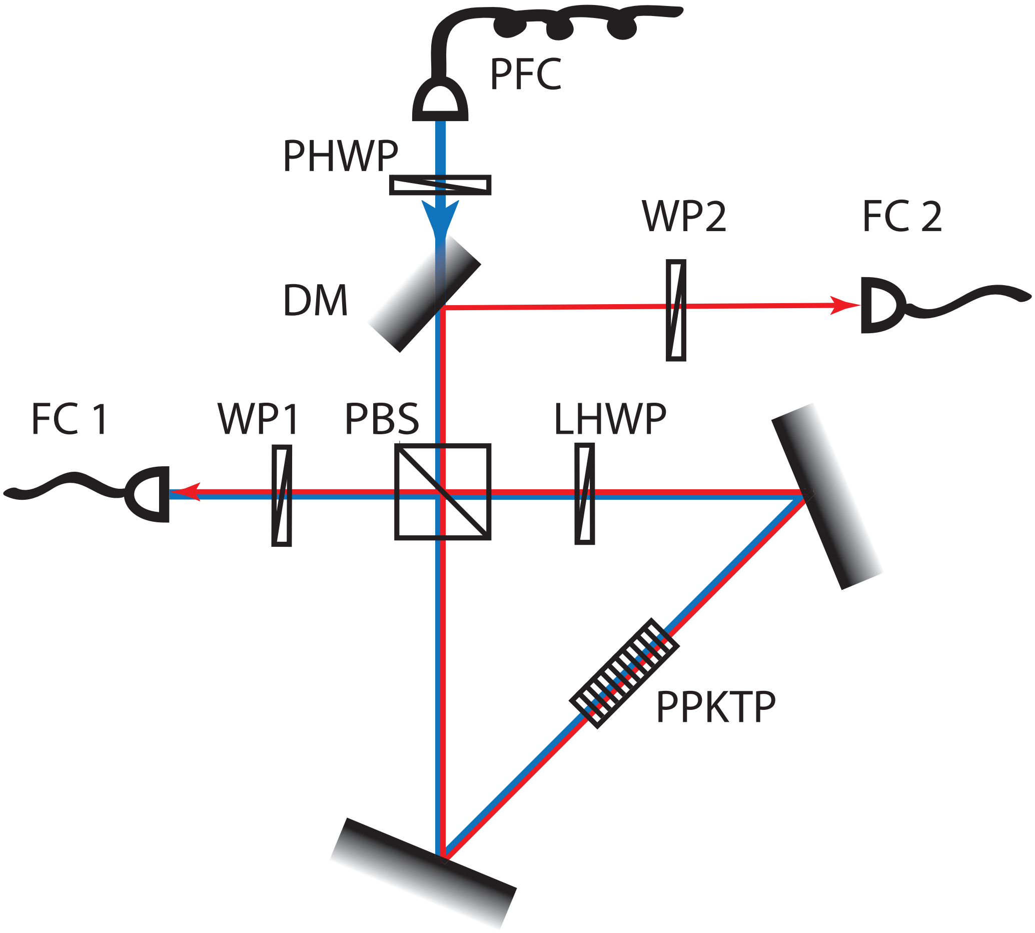

Figure 3.1: A schematic of a simple Sagnac source. Blue lines indicate pump light, red the downconversion modes, or signal. The pump enters the setup from PFC, a fibre coupler, which optimally has a fibre polarisation controller behind it. The pump passes through a half wave plate, PHWP, to control the state being produced—for a maximally entangled state, $|H\rangle \pm |V\rangle$ is optimal, while $|H\rangle$ or $|V\rangle$ generates a separable state. A dichroic mirror is used to insert the pump into the source, which reflects signal and transmits pump. The Sagnac's PBS and loop HWP (LHWP) must be dual wavelength devices, but the performance at the signal wavelength is more important than that at the pump's. The LHWP should be set to rotate horizontal light to vertical for the signal wavelength; if this doesn't quite perform that operation for the pump this can be compensated with PHWP.

The PPKTP crystal in the centre of the loop must be aligned with the counter-propagating beams and temperature controlled. The two outputs from the loop for the signal light pass through some control or measurement optics (here a waveplate (WP), but this depends on the experiment) before being coupled into fibre optic (FC 1,2). The couplers should include filtration to remove the pump from the signal light, either coloured glass or an interference filter; depending on application I switched between either or both of these. The fibre couplers contain the only lenses in the system, which must be carefully chosen. In addition, the couplers should have at least five degrees of freedom (focus and four beam-pointing parameters).

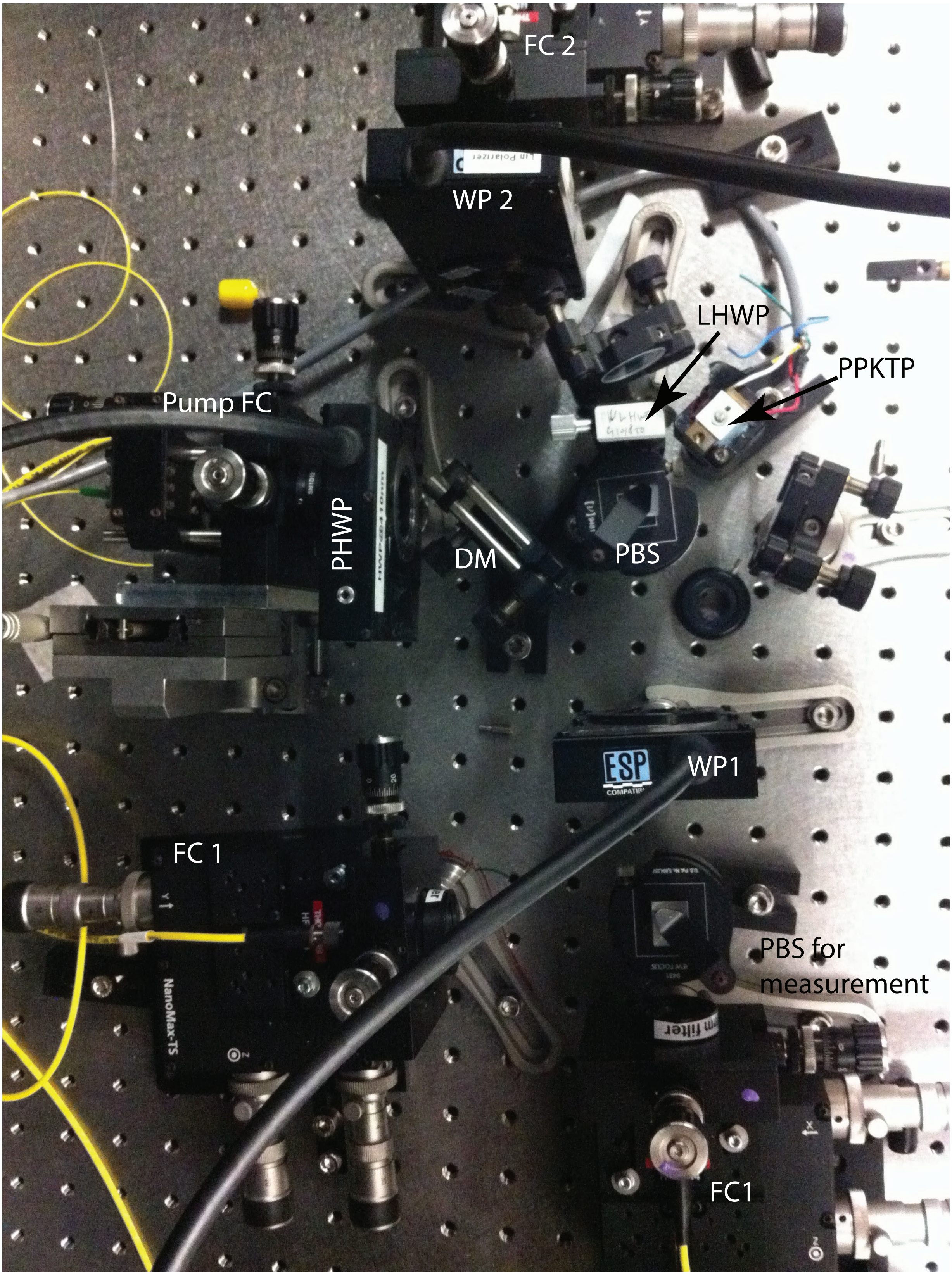

Figure 3.2: A photograph of our source, as used for the Steering experiment. For part labels, see figure 3.1. The extra output fibre coupler is placed to perform a polarisation measurement on the lower output. This diagram is rotated 90°to the left relative to Fig. 3.1.

with A the area of the loop. As our lab is rigidly attached to the Earth, which doesn't spin all that quickly, this can be entirely neglected, and the interferometer simple outputs all of the input light back into the input mode.

This structure is remarkably resistant to vibrations and other disturbances: unless a mirror moves in the time scale of the transit time of the loop (less than a nanosecond for the scales used here), it does not affect the interference[3]. This contrasts with other interferometers such as a Mach-Zehnder, which must be actively stabilised to make photons, and thus perform worse (compare [Fio+04] to [KFW06]).

However, if you simply put a downconversion source inside a simple Sagnac interferometer half of the photons are lost at the beamsplitter. There are two solutions to this that I am aware of being used: the first is to split the photons at the beamsplitter by wavelength with a fairly sophisticated three-wavelength dichroic coating, and the second is to replace the beam-splitter with a polarising one. If the photons are produced in opposite polarisations they are thus emitted in opposite directions, and thus are useful to the experimentalist.

A collinear type-II down-conversion crystal *i.e.* one that generates oppositely-polarised photons—typically periodically poled potassium titanyl phosphate (PPKTP), though periodically poled rubidium titanyl phosphate (PPRTP) also could be used—is thus placed inside our now-polarising Sagnac interferometer.

One more problem must be solved: one of the two pump polarisations reflected from the beamsplitter is polarised orthogonal to that which is phase-matched in the crystal. This is solved using a half-wave plate set to switch horizontal and vertical polarisations, and actually solves another problem simultaneously: it puts both signal photons into one output and the idlers in the other, thus ensuring that they have matching spectra. This actually allows the two photons to not be anywhere near frequency degenerate, which is useful in some circumstances.

3.3.1 Foci

The optimisation of the foci of the three beams (pump, signal, and idler) is a non-trivial problem to solve, both practically and experimentally. First, the easy problem theoretically is the location of all the beams: all of the beams should focus on the centre of the crystal located in the centre of the interferometric loop, and be parallel. On that, everyone agrees and the difficulty lies experimentally: this is easily the hardest part. For the method I used to solve this, see appendix A.

The difficult problem theoretically is to decide how big those foci should be[4]. Until recently

[3] In fact, generally the beams become misaligned before interference is affected by low-frequency motion—these interferometers are *really* stable. Motion on the order of wavelengths/transit time is required to start causing problems.

[4] When I talk about the focus of the down-converted light, I mean the focus that a beam of that wavelength

no one's theory matched experimental results very well; fortunately the move to collinear geometry makes the theorist's life easier and at least two people have seemingly cracked the problem[Ben10; Mit09].

For the experiments of interest here, the performance indicators of interest are the heralding efficiency and the quality of the state, as defined in the next section. This implies, consulting [Ben10], a large pump diameter and a much smaller collection-beam diameter. In fact, I am using the shortest suitable lens available for the pump (3.9 mm), and have tried to match the optimum curve presented in that paper with the down-converted beams.

3.4 Performance

A photon source has several parameters that can be used to quantify performance. Here we are attempting generally to optimise "efficiency" while still maintaining a reasonable quality of entanglement, while we are indifferent to the brightness of the source. Let me quantify all of those terms, then compare this source to others that are available.

3.4.1 Efficiency

The "brightness" of a source of photons is simply the number of photon (pairs) emitted per unit time, useful for quantifying how long an experiment will take, especially one that requires more than one photon[5]. The brightness is not, however, a fundamental measure of performance: it can easily be modified in a number of ways that have nothing to do with the source itself: the most obvious of these being to increase the power of the pump laser, which (in theory) is linearly related to the brightness. Thus, you often see brightness/pump power quoted in the literature. Furthermore, the brightness in this sense is only useful in the regime of stochastically produced light. The actual long-term useful measure of utility is the likelihood that photon(s) are emitted per pulse of the laser (or per clock cycle, to put it in classical computing terms).

This last—the likelihood per pulse of photon emission—is related to another measure of efficiency of a photon source, the "heralding efficiency", η_a. One can in principle make a (deterministic) single photon source from a stochastic pair source by detecting one of the two photons, and then storing the other photon until it is needed. The heralding efficiency is the likelihood that the second photon is present, given that the first photon was detected; that is, given that we detect the idler photon

$$\eta_a = C_{si}/n_i, \tag{3.6}$$

propagating the other direction from that light's output fibre coupler, *i.e.* the spot being looked at by the output of the system.

[5] Note that this is not quite what's meant by the term in classical optics: this is simply power outcoupled, not power per anything.

where C is the number of events where both photons were detected, and n_i the number of events where the idler was detected. It is this figure that will appear in subsequent chapters as a key threshold to several experiments, and (assuming a perfect quantum memory) the 'efficiency' of a stochastic pair source as a single photon source.

Related to the 'heralding efficiency' is the 'symmetric heralding efficiency', η_s: the above measure, symmetrised such that the photons are treated equivalently: this is more useful for symmetric experiments such as a Bell test. This is given by

$$\eta_s = C_{si}/\sqrt{n_i n_s}, \tag{3.7}$$

where n_s is the number of photons detected in the signal mode.

Note that the above measures are all affected by the properties of the detectors used: false positives (dark counts) decrease the efficiency, while both measures of heralding efficiency are upper bounded by the detection efficiency of the system.

3.4.2 State quality

Unlike efficiency, which is simply measured, there are several measures of the quality of a quantum state. If state tomography is used to determine the state being generated, the fidelity (for pure states $F = \langle \text{actual} | \text{ideal} \rangle^2$) to a desired state is a good measure of 'how well did you make what you were trying to make', while measures like the tangle give a good indication of the degree of entanglement or otherwise of the state[6]. For a comprehensive review of such measures, see a review by the Horodeckis [Hor+09].

However, most of our experiments have not had access to full state tomography, as state tomography requires at least three different, linearly independent measurements; in practical terms this implies that at least two waveplates are required in each measurement apparatus. Due to concerns with loss throughout this work there was usually only one waveplate present in each arm.

This leaves us cruder measures of state quality. One, obviously, is simply the parameter that's being measured—a steering or Bell parameter, say. Another, commonly used in the literature, is the entanglement visibility in each of the measurement bases.

The visibility[7], V, of a measurement is [JHS93; JSV95]:

$$V = \left| \frac{\langle ++ \rangle + \langle -- \rangle - \langle +- \rangle - \langle -+ \rangle}{\langle ++ \rangle + \langle -- \rangle + \langle +- \rangle + \langle -+ \rangle} \right| \tag{3.8}$$

[6] The tangle doesn't measure if you made what you were trying to make, just if you made something that's entangled.

[7] The name, and calculation, are derived from the visibility of interference fringes in a classical interferometer

where $\langle\cdot\rangle$ is the expectation value, $\pm$ are the two outcomes of a two outcome measurement, and the two measurements apply to the first and second qubits respectively.

The visibility of a measurement is maximised when the results are highly correlated: this gives a visibility of one. On the other hand, if the measurement outcomes are random (the state is completely mixed or separable) the visibility is nought, giving the familiar $[0,1]$ range of outcomes.

The visibility of a state in one basis merely gives you the degree to which the state is correlated in that basis: in order to demonstrate entanglement correlations in multiple bases are required, preferably ones that are orthogonal. Note that this measure is very, very closely related to the steering parameter, as will be discussed in a later chapter. A maximally entangled state has visibility one in a set of three orthogonal bases; the singlet state $(|01\rangle - |10\rangle)$ has visibility one in all bases.

Chapter 4

Superconducting Transition Edge Sensors

Transition Edge Sensors (TES) are bolometric[1] light sensors that rely on the fast change in the resistance of a superconductor around the superconducting transition for their accuracy.

Initially developed for work with macroscopic amounts of light—and still in use for that purpose today due to their extreme accuracy—their detection regime was extended down to the single photon level by reducing their size significantly, such that the absorption of single photon of light was detectable. Allow me now to explain the design of such single-photon-level optimised TES.

4.1 TES design

The transition edge sensors in use in our experiments were designed and fabricated by the team of Sae Woo Nam at the National Institute of Standards and Technology, Boulder, Colorado, US (NIST). They are 25 μm square by tens of nanometers thick pieces of tungsten, mounted in a dielectric stack (see figure 4.2). This stack is butt-coupled to a single mode fibre optic, held in alignment using the sleeve from an FC-PC fibre-to-fibre connector (see figure 4.1). It turns out that the manufacturing variability in these sleeves is sufficiently small that the alignment of the fibre optic to the detector is trivial—before this method was discovered it was a complicated process involving an electron microscope and person-hours of labour.

These TES are thin films of tungsten comprised of two phases, the bulk phase of tungsten which has T_c about 9 K, while the other, only present in thin films, has T_c about 40 mK. The aggregate's critical temperature depends in a complicated way on the volume fraction of these two phases and is poorly understood but repeatable, yielding a transition temperature of ≈ 150 mK. Lower transition temperatures for the device imply lower noise, but greater difficulty accessing the detection regime. TES can also be manufactured from other superconductors, with

[1] A bolometer is a device for measuring heat using changes in the temperature of an otherwise isolated system.

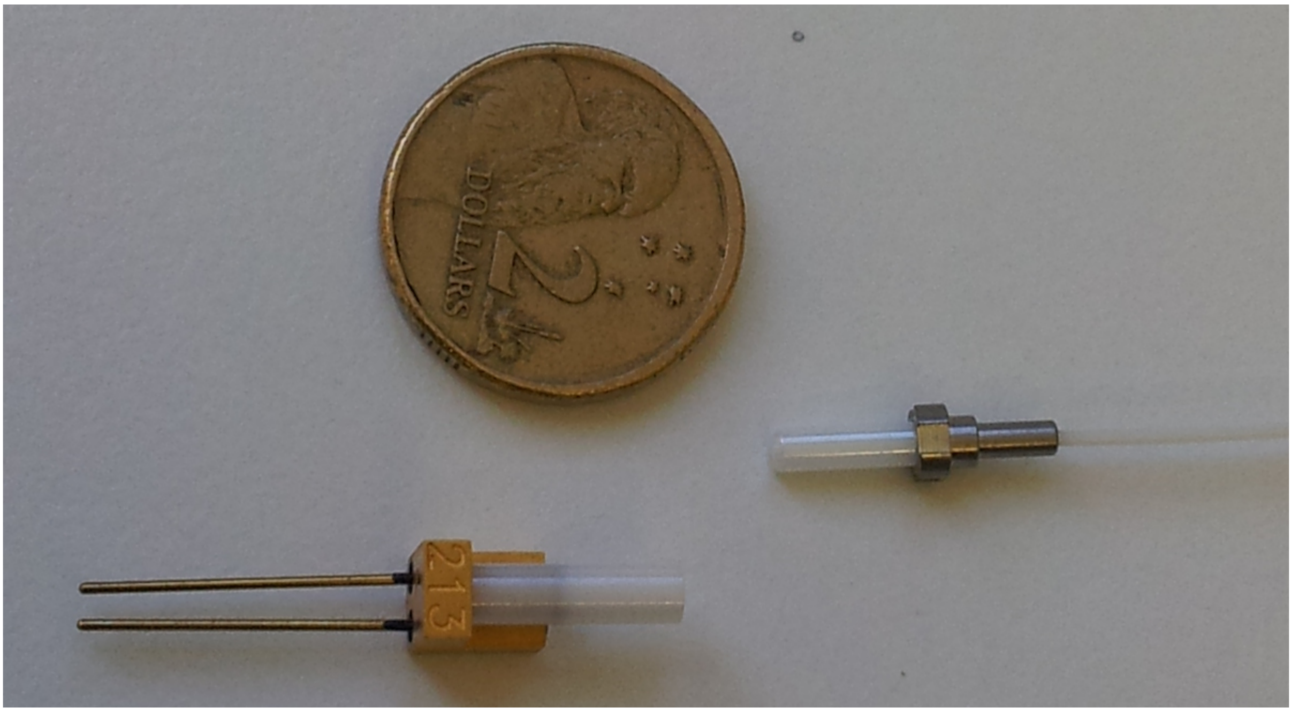

Figure 4.1: A single TES, bottom left, as packaged. The ceramic cylindrical sleeve, white, is fitted over a post, which the silicon wafer that contains the TES is mounted against. The TES connects electrically to the circuit via the two pins emerging from the package, left. Each TES made by NIST is numbered to allow for recordkeeping. A fibre optic, right, can be connected to this TES simply by press-fitting it into the ceramic sleeve as the tolerances on these standard parts is microns; the ceramic sleeve is from a fibre-fibre connector. The $2 coin is for scale.

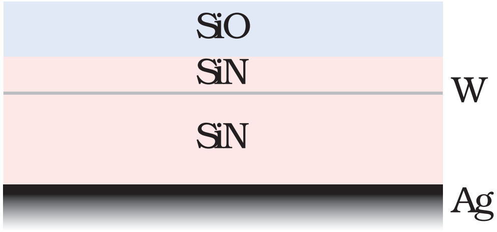

Figure 4.2: An example of the dielectric stack used for TES. The device itself is the thin layer of tungsten (W), which is laid down over a silicon nitride (SiN) layer. Above it, a simple dielectric stack of one layer of SiN and one layer of silica (SiO) is designed to optimise the absorption of light into the TES via the formation of a half-cavity. The back mirror, of Silver, is the substrate for the whole device. In principle a multilayer dielectric back-mirror could outperform the silver as a back-mirror, however in practice absorption in the silver is far from the efficiency-limiting constraint, so this simple system is sufficient. The reflectivity from the device is carefully checked by the fabricators, and if the performance is not sufficient another top layer may be added; I am not sure if that was required for our devices.

titanium devices (with T_c about 8 K) in use: these have sufficiently higher thermal noise to be unable to resolve single photons at telecommunications wavelengths of around 1550 nm.

Since the amplifiers used are magnetically sensitive, as we shall see, a system with low electromagnetic noise is preferable but expensive; for instance liquid helium fridges are much more quiet than more modern pulse-tube designs, but are a pain to work with. Helium also has significant costs either in compressing it back to liquid or in buying new liquid helium. The signal from the detector, measured as a change in current through it, is measured using an array of superconducting quantum interference devices (SQUIDs). These act as Mach-Zehnder interferometers for electrons with the phase of the electronic interferometer set by the magnetic flux through the device—hence the sensitivity to magnetic noise. The current through the TES is transformed into magnetic field through the simple expedient of a small inductor coiled above the SQUID.

4.2 TES operation

4.2.1 How does it work?

The circuit diagram for our TES is shown in figure 4.4, and will be useful to refer to as I discuss the operation of TES.

The sensor itself is held well below its transition temperature[2], and is then biased above I_c, the critical current[3] which causes some amount of ohmic heating to occur. This is effected by applying a voltage bias (at V_{bias} on the diagram) across a large resistor, acting as a constant current source. If the bias current is later reduced, the fact that the device is being heated ohmically will cause significant hysteresis, with the increased temperature reducing I_c, as shown in figure 4.3.

This is the ‘ready’ state for the detector–biased above I_c and thus conducting normally. When light is absorbed by the sensor the energy introduced quickly dissipates as heat in the electron gas, raising the electron temperature and thus resistance significantly. This drops the current through the TES, which reduces the ohmic heating, allowing the TES to recover to

[2] For our devices T_c is about 150 mK while the hold temperature is arbitrarily about 100 mK. Lower temperatures imply lower noise but also shorter hold times, reducing the amount of time the detector is available for use.

[3] For those relatively unfamiliar with superconductors, as I was when I began this thesis, a brief note on I_c. While superconductors have no resistance below some critical temperature T_c, they can only support some amount of current in their superconducting state. Carrying more current than this critical current I_c causes the superconductor's resistance to become finite.

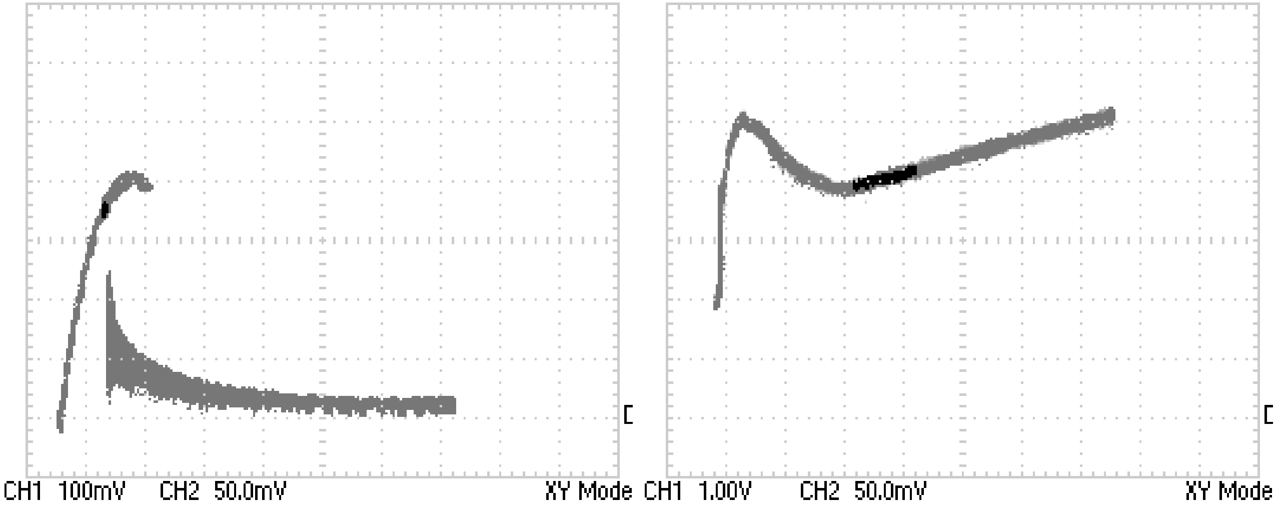

Figure 4.3: The response curves of two of our detectors. The horizontal axes are the bias voltage V_{bias}, starting from 0 V, while the vertical axes are the outputs from the SQUID amp V_{sq}, which is directly related to the current passing through the TES. The steep portion on the left of each curve is the response of the device while supercondcuting, while the region on the right is the normal region.
The difference in their superconducting transition is significant. The left device shows very clearly the hysteresis expected as the current is raised (upper branch), leading to a sudden transition to the normal regime, while as the current is lowered it moves to a significantly lower bias current before it once again becomes a superconductor. This is the expected response for a monolithic superconducting device.
The curve on the right is, however, more typical of our TES. The superconducting-to-normal transition is gradual with increasing bias current. I am not sure of the reason for this behaviour, but I suppose that it is due to the two-phase nature of the tungsten devices. Here the expected hysteresis does not appear at all.

its initial condition, as much current is shunted through the 10 mΩ resistor in parallel[4]. The electron gas is coupled weakly to the phonon bath in tungsten, allowing an additional path for heat to dissipate—this is slow in comparison to the drop in ohmic heating, however. One advantage of tungsten for TES is that the electron-phonon coupling *is* low, as heat transferring from the electrons into phonon modes is a source of noise. The ideal bolometer is completely isolated from its environment except for paths deliberately introduced by the user.

The current through the TES is measured inductively with an array of superconducting quantum interference devices (SQUIDs)—one of the many unfortunate names bestowed upon something that's entirely unenlightening. A SQUID is a loop of superconductor—in this case Niobium—interrupted by two (or more) Josephson junctions[5]. The two electronic paths around the loop, each through a junction, interfere in a manner equivalent to a Mach-Zehnder interferometer for photons; the phase of the interference is set by the magnetic flux through the loop, with the visibility of the interference controlled by the voltage across the SQUID. In our system, this is set by a bias voltage on the positive terminal of the output amplifier.

This interference effect can be used to amplify small signals–small changes in magnetic field can lead to large changes in the current through a SQUID if the initial phase of the interferometer is on the steepest part of the fringe; unfortunately this only holds for an input phase change much smaller than a single interference fringe. One problem arises from experimental constraints: In order to get a large enough signal given other constraints we must use an array of SQUIDS in parallel. As long as the devices' phases are all the same, this is transparent to the user, but if the SQUIDs are driven out of the superconducting regime ('become normal') during operation (usually by putting too much current through them, via, for instance, a short circuit) they may dephase as they cool back into the superconducting regime, reducing the available amplification.

The TES is in series with a small inductive coupler, the loops of which are overlaid on the SQUID array. (While an inductor is inimical to fast responses, SQUIDs are lower-noise amplifiers than are otherwise available.) The current response of the TES thus directly translates to the phase of the SQUID; the range of the TES's current is sufficiently small that the response is approximately linear, *i.e.* much less than a quarter fringe. However, in order to get that

[4] The power dissipated in the TES due to ohmic heating is approximately

$$P = \left(\frac{I_{\text{bias}}}{R_{sh} + R_{\text{parasitic}} + R_T} \right)^2 R_T,$$

where R_{sh} is 10 mΩ, the parasitic resistance is about 50 mΩ, and R_T is the TES's current resistance. This drops when the resistance rises, quickening the recovery time.

[5] A Josephson junction is nothing more than a small piece of insulator between two pieces of superconductor across which Cooper pairs of electrons can tunnel with no resistance, a sufficiently surprising state of affairs as to be worth a Nobel prize. They do not introduce resistance, but the AC phase across such a junction is changed.

linear response the SQUIDs' phase must be held at a sensitive point, which is done by means of the poorly-named 'feedback' circuit.

The 'feedback' circuit[6] to the SQUIDs is nothing more or less than a variable voltage source across a 5.2 kΩ resistor with another inductive coupler to the SQUIDs, this one with 10 times as many turns[7] as the TES channel's. Adjusting the source voltage easily traces out an interference fringe of the SQUID, allowing the phase of the 'ready' state to be optimised to the steepest part of the fringe—this maximises the signal size of photons absorbed in the detectors as they deviate from this initial position.

4.2.2 Cryogenics

In order to keep transition edge sensors in their superconducting state, some cryogenic system is required. Our TESs are kept in an adiabatic demagnetisation refrigerator (ADR) backed with a pulse tube refrigerator. While neither of these technologies is core to this thesis, I'll spend a moment of your time giving a brief description of them.

To maintain any kind of cryogenic temperature a vacuum is required—air would liquify well above the temperatures discussed here. Our fridge is a commercial product[8], which we evacuate using a turbopump. Once cryogenic temperatures have been reached the system is sealed off from atmosphere as there is no point in pumping air out of a box that the air has frozen to the sides of. In fact, the pump would allow air to flow into the vacuum system at that point, where it would freeze onto various surfaces. This 'cryopumping' of the system brings the base pressure to about 10^{-7} torr.

A pulse tube refrigerator operates on the same principle as a standard house fridge, just on a colder scale. Helium under pressure is pumped into a low-pressure volume and allowed to expand, cooling as it does so. It's then pumped out of the expansion chamber and repressurised. Two such pulse tube refrigerators are operated back-to-back in our system, the first cooling to 50 K and the second to approximately 4 K (using the 50 K stage as the hot side and heat dump for the second cooler). In the past this part of the system would be replaced with liquid helium cooling, however the recent rise in the price of helium has made alternatives such as this one economically preferable. Unfortunately, 'wet' fridges have significantly lower electromagnetic noise than these newer systems, adding to the complexity of the project.

The SQUID amplifiers are kept at this 4 K level. Their critical temperature of around 9 K is well above the temperature of this stage, while thermal noise is sufficiently low. Experi-

[6] The feedback circuit is so named because in TES systems with substantially larger (macroscopic) signal sizes this actually feeds the signal back to the SQUID to maintain the linear regime. Here the feedback is strictly open loop.

[7] Sae Woo Nam, private communication

[8] High Precision Devices, Inc., Colorado, USA

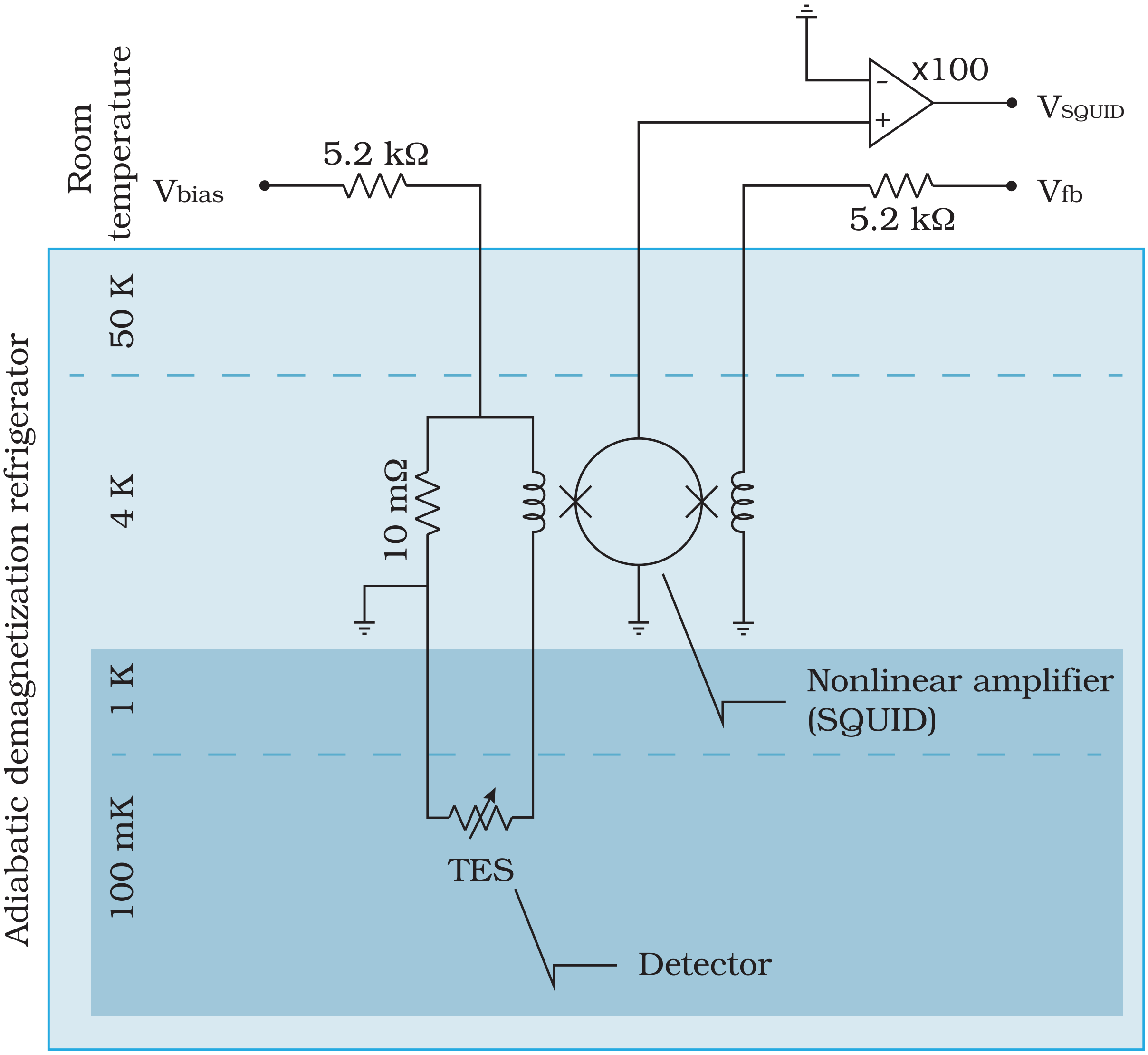

Figure 4.4: TES circuit and associated components. Three connections are available to the experimenter, operated as two inputs and one I/O line. V_{bias} is used to set the TES to the correct operating point. V_{fb} sets the SQUID to its most sensitive position, and a bias on the amplifier on the V_{SQUID} terminal affects the visibility of the interference fringes in the SQUID array. The output is measured through an amplification circuit on the V_{SQUID} output via a discrimination circuit (see figure 4.5) . The various stages of this circuit are held inside our cryosystem, with the temperature levels shown at left; all electrical connections are twisted pair, with the ground plane of the circuit at room temperature.

ments have been done with the SQUID amps cooled further—to approximately 1 K—to reduce the noise further, but this reduces the hold time of the system and is of marginal benefit to performance.

The final stages of cooling is done using an adiabatic demagnetisation refrigerator (ADR). Here a large electromagnet is run to full field while a magnetic salt is held inside it attached to the heat bath. After the salt's thermal link to the heat bath is removed, the field is slowly reduced to a much lower value, allowing the 'adiabatically demagnetisation' of the salt. As entropy is conserved during this process, the increased disorder in the salt due to the magnetic domains misaligning is extracted from the thermal energy of the solid, reducing the temperature significantly. This process is a single-shot process in the sense that the cold stage cannot be continuously kept cold; after the magnet reaches zero field the whole process must begin anew, requiring at least 90 minutes to magnetise the salt and allow it to thermalise.

Our ADR's magnet is made of superconducting niobium wire and supports a magnetic field of about 4 T at a maximum current of 9.3 A[9]. The magnet circuit's resistance is about $1/8\,\Omega$, mostly from the lead wires, while the inductance is about 33 H: This is where the numbers start to be really strange, as typical inductances for inductors you might put in a circuit are in the nanohenry range. Given that this magnet is over a kilometre of wound wire, this shouldn't be surprising, but it's still disconcerting, and causes control system issues as we will see later.

Due to the amount of wire and current involved, 'quenching' the magnet is a serious concern: if the wire goes normal (*i.e.* not superconducting) for any reason there is a substantial amount of heat dissipated. In our fridge, there's three ways that this could happen: First, too much load could be put across the magnet as it's being turned on, with 'too much' being about 2 V;[10] second, a power failure could cause the power supply to switch off, dumping the current and putting a large negative voltage across the magnet[11]; or the obvious third option of the magnet rising above its transition temperature. The first two problems are mitigated by emergency shunt diodes mounted inside the fridge, but are still to be avoided, while the primary cause of temperature rises are also power failures: hopefully any power failure that switches off the fridge also switches off the power supply to the magnet gracefully. A sufficiently severe quench can actually heat magnets like this one above their melting point ($\sim 2500°$C), ruining the magnet: this is Very Bad.

The power supply for the magnet is another critical piece, as it both controls the temperature of the system at low temperature and has to drive the much larger scale magnetisation cycle without failure. We use an Agilent constant current/constant voltage supply controlled by

[9] The bizarre numbers that come about with superconducting wire hit home about here for me. What other circuit are you happy about drawing 9-odd amps of current?

[10] As a matter of rule our magnet is kept below 1 V between its leads.

[11] This has happened to our magnet due to, as I recall, some construction work. A few nervous days ensued.

a PID[12] controller, which in turn is controlled by a computer during the magnetisation and demagnetisation cycles.

Setting the PID controller turns out to be tricky—our power supply has a capacitor protecting the device, and for most circuits this is nearly invisible as a typical circuit is capacitive/resistive, but for our system comprising for the most part a large inductor it poses a problem, turning the circuit as a whole into an effective LC circuit, with the small lead resistance providing damping. The resonance frequency is about $\omega \equiv \sqrt{1/LC} \approx 1/3\,\mathrm{s}^{-1}$ with $Q \approx 10^4$. Commercial PID units' timescales are significantly smaller than the resonant frequency, and will thus tend to over-control this system. In order to get good stability our PID controller is set to nearly minimal P and I, and D is turned off.

This problem can be somewhat averted by putting more resistance in the circuit when in low temperature operation, but doing so makes it harder to automate the process. As-is our system is quite stable, but has a persistent 3 mK offset between set temperature and the actual temperature due to insufficient integral control[13].

4.2.3 Digitisation and counting

At the exit from the fridge the signal from the TES is about 1 mV in magnitude, and must be further amplified before it can be used. The first stage of additional amplification occurs in custom 10× amplifiers that also provide the bias on the SQUID circuit. These currently are a standalone module for each detector, but an integrated 8-channel device should be installed imminently.

The signals are then fed to a commercial amplifier and amplified a further 10× before being digitised using a constant fraction discriminator (CFD). A CFD, if set up correctly, "clicks" at a constant fraction of the height of a pulse, rather than at a particular voltage level, as in a threshold discriminator. For pulses of constant rise time but variable height, this reduces the variance in the timing information; our pulses are in this category to within experimental error independent of photon number.

Unfortunately, CFDs are designed for much faster pulses than the ones output by a TES, which have a rise-time of tens of nanoseconds. A delay line with approximately the rise time of the signal is required for the operation of a CFD, and in our case this delay line is approximately 10 m of coaxial cable. This is both fairly attenuating, and far outside the spec of the CFD, making them operate less perfectly than one might hope. A further constraint is that the CFDs do not allow for number resolution of the signal, merely threshold detection at some number of photons present (*i.e.* one or more, two or more, &c.). For a detailed look at the circuit for one

[12] Proportional, Integral, & Derivative feedback

[13] I think so, at least: a previous round of calibration did not have this offset, and I'm not sure why.

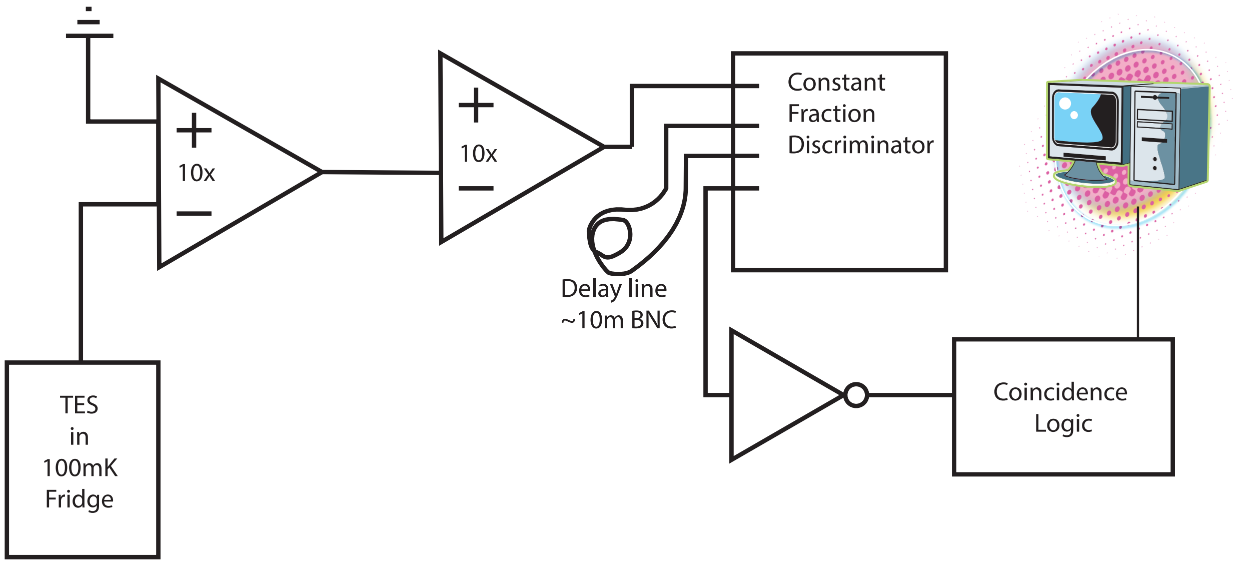

Figure 4.5: A sketch of the electronic setup for each TES. The signal coming out of the fridge is first amplified by a custom low-noise 10x amp, which also provides the bias current for the SQUID amp. That is then amplified to about 15 mV by a second 10x differential amplifier, *n.b.* that the input chosen to the second diff amp varies depending on the tuning of the SQUID amp to ensure the that the sign of the signal input to the CFD is correct.
The signal is then fed to a constant fraction discriminator, which then outputs the pulse inverted into a delay line. This line should be about the length of the rise of the signal, which turns out to be about 10 m of BNC cable, which unfortunately but unavoidably attenuates the signal. The logical output of the CFD is in negative-going NIM[14] logic, while our coincidence logic (from IQOQI, Austria) requires positive-going TTL[15] pulses, so a NIM NAND gate is used to invert the pulse as it has a TTL-levels output. The coincidence logic has 2.56 ns timing discrimination, and can monitor up to 64 patterns of coincidence between the eight inputs. It in turn talks to a PC running LabView to be monitored and recorded.

TES, see figure 4.5.

Geoff Gillett, in our research group, is working on a system, based on a field programmable gate array (FPGA), that digitises the signal directly and then analyses it, obviating the need for CFDs.

4.3 Performance

Transition edge sensors have a quantum efficiency that is experimentally indistinguishable from unity, but this is not a fair indication of the total efficiency of the devices (nor is it for other possible detectors, despite the quantum efficiency being bandied about). The quantum efficiency of a detector is the chance a detection will be registered *given* that the photon was absorbed in the detection medium. A bit of thought will make it obvious that getting the photon absorbed in the detector is also a major problem, and when the quantum efficiency approaches one is the major problem.

Because TES are a thin metallic film, early TES had problems with light passing through the device. Fortunately, with a silver back-mirror and a simple dielectric stack (and a bunch of clever engineering) Sae Woo Nam's group at NIST have raised the turn-key efficiency of the detector package in excess of 95% [LMN08]. Private communications with their research group indicate that values in excess of 99% have probably been achieved at some point, but measurement difficulties, particularly a very good understanding of systematic errors, make reporting such efficiencies difficult, which are measured using a carefully attenuated laser. An alternative approach, known as (quantum) detector tomography using single photons may provide better answers in future[Lun+09].

Another good piece of work on a similar system (titanium rather than tungsten TES) by a group in Japan has showed that the detection efficiency for each subsequent photon at the same time is very close to linear [Fuk+11]. That is, given that there is an efficiency of η for detecting a single photon (Fock state); for a biphoton the probability of detecting is as such is η^2, and with probability $2\eta(1-\eta)$ it is detected as a single photon. Therefore, the detection efficiency for multiple photons is effectively independent of the number of photons present until saturation is reached. There is a trade-off between performance characteristics, with energy resolution and saturation levels trading off; the detectors in use here begin to saturate at 6-10 photons. This contrasts with most other detection technologies, which are either completely incapable of resolving photon number, such as SPADs[16], or start to saturate or miss photons before the device is completely overwhelmed.

However, that's still not the whole story. Our TES, at least until after the majority of the results of this thesis, were coupled to SMF-28e fibre optics, which are standard fibre optics for telecommunications, and are single mode at 1550 nm, with a cutoff frequency such that they are bimodal at our single photon wavelength of 820 nm.

This leaves two options: one can couple the light into those fibres directly and hope that the second mode does not cause problems, or one can couple light into fibres that are single mode at 820 nm and then transfer the light somehow into the SMF-28e fibres.

While another research effort[Ram+12] found success with the method of coupling directly into SMF-28e, our own comparative data indicated that the other approach was more likely to succeed in reaching very high efficiencies. The difficulty in using the SMF-28e directly is that the additional propagating modes present in the fibre allows unwanted light to couple more easily, increasing noise and thus decreasing the heralding of the source[17]. The solution chosen

[16] It is in principle possible to get some photon number information from SPADs by comparing the size of the avalanches and trying to find the size of the snowball that started them. This is about as hard as it sounds, and is incredibly noisy. For tomographic purposes, however, it should in theory be sufficient.

[17] I have not seen the analysis from Vienna on how they reached the opposite conclusion. I would be interested

for my experiments, then, was to couple light directly into anti-reflection coated SM9/125 fibre, a fibre that is single-mode at 820 nm, and then splice that fibre directly to the SMF-28e fibre in as low-loss a way as possible given the technology on hand. This resulted in loss of about 0.09 dB in the splice, as measured using a calibration laser beam, and also as estimated by the fusion splicer itself[18]. Better performance is in principle possible for such a splice if the change in mode field diameter between the two fibres is adiabatic rather than abrupt, but fusion splicers capable of such work were not available at the time.

'Dark counts', or false positive events, plague some other detection technologies. Fortunately, on our TES these are indistinguishable from zero: however, stray light remains a problem. Our source was enclosed in an aluminium box, and the fibres kept in opaque tubing to try and reduce stray light coupling to the detectors. Moreover, when experimental runs were being taken the lights in the laboratory were kept off. The background false positive rate was about $8\,\mathrm{s}^{-1}$.

The last two performance characteristics of a photon detector are to do with timing: the dead time after light is detected before another event can be seen, and the timing uncertainty of the detections. The latter can be measured by taking a histogram $t_1 - t_2$ for nominally coincident events on two different detectors[19], such a histogramyields a timing jitter of $\Delta t \approx 33$ ns for each detector. This uncertainty arises from several sources of varying importance: it was conjectured that a primary cause was the response of the detector itself; however recent experiments from NIST indicate that the parasitic inductance of the twisted pair connecting the TES to the SQUID amp was a dominant source, as eliminating it reduced the timing jitter to approximately 4 ns [LL+13].

The dead time of TES is in principle very close to zero: the rise in resistance is in some sense independent of the baseline resistance, so even while the detector is recovering to base temperature another spike in resistance is measurable. In fact, the in-principle limits to detection rates are saturation of the detector medium and the timing uncertainty of the detector: differentiating between two photons at once and two photons consecutively inside the timing window is difficult.

In practice the dead time is set by the ability of the discrimination electronics to differentiate pulses. Our CFD-based system is unable to detect such overlapping pulses, and so goes dead to avoid false positives of various kinds due to electronic noise, with a dead time of about 0.5-1 μs depending on the particular detector and tuning of the CFD.

to, but it doesn't appear in their published work at this time.

[18] In some experiments, including the steering experiment, one of the photons was fibre coupled, send through another set of bulk optics, and then fibre coupled again. In this case, the second fibre was SMF-28e, since the primary source of noise from using such fibres is photon pairs created with non-ideal parameters in the source.

[19] Conveniently/unfortunately, the timing uncertainty in photon pairs from spontaneous parametric down conversion is negligible compared to the timing uncertainty of these detectors.

The CFD dead time sets an unfortunate upper bound on the rate of experiments which is lower than is immediately apparent; to wit, given the design goal of high-efficiency experiments, this dead time causes problems in the following way: imagine a photon pair is emitted by the source, and one of the two photons is detected whilst the other is lost. Then, another photon pair is emitted by the source within the detector dead time. For this pair, one of the two detectors has an effective detection efficiency of zero, so once again at most one photon can be detected. At high count rates this condition can persist indefinitely, while even at lower count rates every such event reduces the apparent efficiency of the detectors used in a one-to-one ratio.

Chapter 5

Quantum Steering

Quantum steering, otherwise known as EPR-steering or 'the EPR criterion for entanglement', is a task first proposed by Erwin Schrödinger in 1935 [Sch35]: that of convincing an unbelieving party of the existence of quantum entanglement. Consider the following scenario, wherein Alice tries to convince Bob of entanglement:

1. Alice sends Bob a (quantum) system
2. Bob tells Alice how he's going to measure the system
3. Alice tells Bob what his measurement outcome will be
4. Bob measures the system

If Alice sufficiently often successfully predicts Bob's measurement outcome, this experiment is incompatible with the predictions of classical mechanics and requires Bob's system to be entangled with Alice's [WJD07]. The exact details of the measurement Bob chooses, as well as exactly how often 'sufficiently' is, depend on the exact details of the protocol. As a brief aside, Bob's state unconditioned on Alice's remains unchanged, thus this protocol, and others like it, does *not* violate the no-signalling principle.

In this chapter, I will be discussing our results from our experiment in steering, published in Nature Communications [Smi+12] and included as Appendix C to this thesis. I strongly recommend that a reader unfamiliar with the paper in question read the Appendix before continuing with this chapter. I will briefly recap the results of that paper, and discuss some topics that failed to fit in the paper, such as other possible choices of protocol and how they affect the analysis, as well as a comparison of our results to those of several other research groups worldwide: three groups were working in parallel on this problem at the time, with the complementary results from the other groups found at [Wit+12; Ben+12]. Prior to those results, all experimental tests of non-locality (steering or Bell inequalities) with single photons were post-selected, allowing cheating by hiding unfavourable events in losses.

The source and detectors in the paper have already been discussed in this thesis, while the experiment itself is actually remarkably simple except for the problem of requiring high efficiencies, consisting of a few waveplates and polarising beam-splitters. We report a then world-record 62% asymmetric heralding efficiency[1].

5.1 Steering Inequalities

The steering inequality we use, quadratic in the measurement outcomes, is

$$S_N \equiv \sum_{i=1}^{N} E\left[\langle B_i\rangle_{A_i}^2\right] \leqslant 1, \tag{5.1}$$

where A_i and B_i are Alice's and Bob's measurement results for the ith measurement basis, which must be mutually orthogonal. Bob's measurement outcomes are given by ± 1, corresponding to measurement in his two detectors, while Alice may output ± 1 or 0 with no restriction (see below). $E[\cdot]$ is Bob's conditional average expectation, defined as

$$E\left[\,\langle B_i\rangle_{A_i}^2\,\right] \equiv \sum_{a=\pm 1,0} P(A_i = a)\,\langle B_i\rangle_{A_i=a}^2\,,$$

where $P(A_i = a)$ is the probability that Alice's measurement result is a. and $\langle B_i\rangle_{A_i=a}$ is Bob's expectation value in basis i given that Alice's result is a. For each measurement basis, $E[\cdot]$ ranges from 0, if Alice's measurements are uncorrelated with Bob's, to 1 if they are perfectly correlated.[2]

Note that A_i is allowed to take three values, while B_i has only two: when Bob successfully measures a photon (his detector 'clicks') he demands from Alice her corresponding measurement result, per the protocol above. In principle, her responses come from a black box; in practice she outputs a measurement if her photon reached her and otherwise outputs zero. This gives equivalent results to other solutions to the real-world-loss problem, but is the most explicable. Other potential solutions include forcing Alice to make a choice amongst binary outcomes for each of Bob's measurements, and allowing an explicit 'no result' outcome for Alice that is not factored into the steering parameter, but modifies the threshold instead.

If Alice's and Bob's inputs are unentangled, $S_N \leqslant 1$ independent of N, as Alice's optimal strategy is to send Bob a single pure state equidistant between one of his measurement out-

[1] Since surpassed by [Giu+13; Chr+13], amongst others.

[2] Or anticorrelated, due to the square

comes in each bases; *e.g.* Alice can choose the $|+\rangle$ outcome for each basis and send Bob the superposition thereof. This gives the maximum overlap between Alice's knowledge of the state and the actual measurement outcomes Bob receives—for a mathematical proof by Cyril Branciard, see the methods section of Appendix C. Thus, in order to violate a steering inequality at least two bases must be used, as any old classical system can be correlated in one basis, it's when things are correlated in incompatible bases that things start getting quantum. As this inequality requires orthogonal measurement bases the upper bound on N is three. We made the obvious decision, given our capabilities, to perform the experiment with both N equals two and three.

The question to ask before trying one of these inequality experiments is 'how hard is this going to be?'. One possible way to analyse this is to look at 'how badly can we do things?'. The two parameters I choose to work with here are the visibility of entanglement (post-selected) and heralding efficiency, and I'll analyse the all the non-locality experiments presented here in that light. We assume for the purpose of this analysis that the state emitted by the source is a Werner state

$$\rho = V(|01\rangle - |10\rangle)(\langle 01| - \langle 10|) + (1-V)\mathbb{I}_4/4.$$

This state is a mixture of the state intended with the four-dimensional completely mixed state $\mathbb{I}_4/4$; mixture with the completely mixed state is in some sense the worst error—depolarisation—possible.

The degree to which this state approximates the actual experimental one is questionable, but the results are illuminating nonetheless. In particular the fringe visibility in the photon's creation basis $\{|0\rangle, |1\rangle\}$ tends to be higher than that of rotated bases, and the $|10\rangle$ and $|01\rangle$ terms are usually not quite identical either. However, with suitable averaging the visibility numbers from the lab can be plugged into these inequalities for useful results without complicating the mathematical model overmuch.

For the quadratic steering inequality we can violate the inequality iff:

$$\eta V > 1/N, \tag{5.2}$$

as for each of the measurement bases we can attain a maximal value of V on positive measurements, and those constitute η of Bob's total measurement outcomes; multiply by N bases and the final outcome is reached.

One final note before moving on to another steering inequality: Bob's measurements—both the bases and the outcomes therein—are constrained to be orthogonal by the structure of the proof of this inequality. Considerable effort was made in this experiment to ensure that condition was met insofar as possible, and a correction was made to the bound of unity to account for the remaining errors.

Another steering inequality, this one linear in the measurement outcomes, has been developed in recent years[Ben+12; Sau+10], is

$$\mathcal{S}_N \equiv \frac{1}{N}\sum_{i=1}^{N} \left\langle A_i \sigma_i^B \right\rangle \leqslant C_N(\eta), \tag{5.3}$$

where $\mathcal{S}$ is this, different, steering parameter, σ_i^B is the Pauli operator for Bob's ith basis. Note that $\left\langle A_i \sigma_i^B \right\rangle$ is effectively the post-selected visibility in the measurement basis $i.C_N(\eta)$ is a parameter that depends on Bob's number and choice of bases and Alice's reported loss η that represents the optimal non-entangled (or 'classical') value of $\mathcal{S}_N$[3] In the high efficiency limit ($\eta = 1$)

$$C_N(1) = \max_{\{A_i\}} \left\{ \lambda_{\max} \left(\frac{1}{N} \sum_i A_i \sigma_i^B \right) \right\}, \tag{5.4}$$

where $\lambda_{\max}(O)$ is the maximum eigenvalue of the operator O. That is to say that, in the absence of entanglement the steering parameter can be maximised by emitting a pure state and guessing the most likely outcome for each of Bob's bases. This pure state should be chosen such that the correlation is maximised over all the bases chosen.

If Alice is allowed loss (*i.e.* $\eta < 1$), C_N increases, as the untentangled optimum strategy can use loss to omit 'bad' outcomes from the steering parameter by outputting a loss event instead. In particular, the naïve deterministic strategy is to optimise the pure state found via equation 5.4 over only over $M < N$ of the bases chosen and output a 'loss' of the photon if another basis is chosen by Bob. Thus, for instance,

$$C_2\left(\frac{1}{2}\right) = 1, \tag{5.5}$$

as Alice emits a pure state that is an eigenvector of Bob's measurement in one basis, and tells him she lost the photon when he wants measurement results in the other basis[4]. This deterministic strategy obviously only holds for $\eta = M/N$, and in fact is not necessarily optimal even then for all choices of M and N.[5]

The optimal strategy for Alice does, however, correspond to a weighted mixture of these

[3] Compare the limit on S_N, which was unconditionally 1 in our formulation. Effectively, for the quadratic inequality $C_N = 1$, and Alice's inefficiency is absorbed into S_N.

[4] Obviously in a real-world application she should choose one or the other basis to align with at random for each trial to avoid detection.

[5] Bennet *et al.* [Ben+12] in fact show that for $N = 10$ the $M = 4$ strategy is never optimal for their choice of 10 bases, which is the most-symmetric set they could come up with (the measurement eigenvectors form an icosahedron on the Bloch sphere).

optimal deterministic strategies[6]:

$$C_N(\eta) = \max_{\{w_M\}} \left[\sum_{M=1}^{N} w_M C_N \left(\frac{M}{N} \right) \right] \tag{5.6}$$

such that $w_M \in [0,1]$, $\sum w_M = 1$, and $\sum w_M M/N = \eta$. Not more than two of the w_M are nonzero, though they do not necessarily correspond to adjacent values of M[7]; however $\binom{N}{2}$ is an easily searchable space for practical values of N.

If Bob sets additional constraints on Alice, such as requiring her efficiency in all bases to be equal, that can only reduce her effectiveness: thus I can neglect such constraints and simply violate this optimal C_N. Note that this whole steering inequality is task-oriented, rather than a deep philosophical insight into steering as a concept. Alice is attempting to convince Bob that they share entanglement, and in order to do so Bob computes her optimal unentangled strategy (given by C_N). This is far from the only way to frame this task–another is as a game that Alice wins by successfully predicting Bob's outcomes, and so on.

The linear inequality represents a recent re-framing of the steering task with some advantages over the older quadratic one: The linear steering inequality is more flexible than the quadratic option, as the bases are not constrained to be orthogonal, allowing the number of such bases to increase without limit. This additional flexibility on the part of Bob makes Alice's task, in general, more difficult, allowing this steering inequality to, in the limit of infinite bases, tolerate arbitrary losses.

Moreover, this linear steering inequality outperforms the quadratic one in our paper unequivocally: while the thresholds for minimum visibility or efficiency remain the same, the tradeoff between them is better, including more states in the steerable set while excluding none.

As a side issue it should be noted that these analyses treat Bob's measurement as a projective one, and have no room for him to instead implement a positive operator-valued measure (POVM), otherwise known as a 'generalised measurement', which is the generalisation of the projective measurement to the case of non-orthogonal and overcomplete outcomes.

There exists yet a third class of steering discussions that has made a splash in the literature, from Wehner and Oppenheim's [OW10] paper showing that the degree of nonlocality in quantum mechanics is limited only by the uncertainty principle. They show that 'non-locality' of a theory is constrained by two things, the uncertainty of incompatible measurements and the steerability of the theory in the sense we are discussing here. They discuss which states can be steered to, rather than discuss inequalities that demonstrate that steering as I'm using here: that is, in

[6] I'm not going to prove that, but it follows from linearity. A slightly larger argument is present in [Ben+12].

[7] They are smooth, however: as a particular value of M that *is* used is passed through the optimal strategy shifts from between two different mixtures of C_M with another C, with a point at exactly $C_N(M/N)$. However, not all $C_N(M/N)$ are optimal.

terms of remote state preparation with certainty. As was remarked remarkably often during the experiment and preparation of the paper thereafter: Steering is remarkably close to remote state preparation in concept and execution[Kil+10]. If steering is treated as a game, where Alice wins if she can predict Bob's measurement outcomes, a state is 'steerable' for Oppenheim and Wehner iff she can win with certainty if she gives (some of) it to Bob and he has free choice of measurement basis[8].

Consider an arbitrary, not necessarily quantum-mechanical, state for Bob: $\sigma_B \equiv \mathrm{Tr}_A(\sigma_{AB})$. σ is being used for the state variable because Oppenheim and Wehner did not constrain their discussion to quantum mechanical assumptions. In a quantum setting, these are (reduced) density matrices. My apologies for the confusion with Pauli matrices in the prior discussion.

Then, so long as the state space of the part of the state belonging to Bob is convex his part of the state can be expressed in many different decompositions. Here we express it as a decomposition over measurements made on Alice's side A_i and its outcome i:[9]

$$\sigma_B = \sum_{A_i} p(A_i|i)\sigma_{i,A_i}. \tag{5.7}$$

Here $p(A_i|i)$ is Alice's probability of outcome A_i given measurement i; thus for measurement i there is a $p(A_i|i)$ chance that Bob's state is σ_{i,A_i}. Since the partition of Bob's state into various pices disappears when the conditioning on Alice's outcome is lost, this steering doesn't violate the no-signalling condition[10]; however, Alice gains information over Bob's state by her own, remote, measurements.

In fact, Schrödinger noted that for all possible ensembles for which equation 5.7 holds there exists a bipartite quantum state σ_{AB} and a set of measurements A_i allowing Alice to create that ensemble. That is to say: quantum mechanics saturates steerability. No other theory can possibly have more steering without violating the no-signalling principle.

Classical mechanics, as we have seen above, does not saturate steering, limiting its nonlocality despite its lack of uncertainty. Oppenheim and Wehner's [OW10] paper does not derive an inequality for steering, (and indeed does not quantify less-than-perfect steering at all, considering only the set of states for which perfect steering is possible rather than the amount of steering allowed on a given state in an arbitrary system) but I think their approach is enlightening[11]

The thesis of Oppenheim and Wehner's paper is as follows: nonlocality, or the degree to which events can influence distant events outside the future light cone, is ultimately constrained

[8] Bob is constrained to projective measurements, not POVMs.

[9] *n.b.* I have changed the notation of all three of these steering concepts to maximise clarity.

[10] The no-signalling condition is the constraint that no information can be transmitted superluminally. This is assumed to be true, and is the sense in which the universe is local (or not too non-local, at least, depending on your philosophical position).

[11] I have talked to Prof. Wehner about their result, and since their definition is maximally general our steering results confirm greater-than-classical steering in quantum mechanics in their framework.

by a relationship between two things. First, the mutual uncertainty of the theory—the degree to which different measurements can all be definitely specified: classical mechanics has no uncertainty, while quantum mechanics and local hidden variable models have progressively more. Second, the steerability of the theory—the degree to which measurements on a local system can predict measurements on a distant, noninteracting system: quantum and local hidden variable models have perfect steerability and classical mechanics has less.

The nonlocality, as measured by a Bell-type inequality, of local hidden variable and classical models is the same, showing that LHV models trade off certainty for steerability. Quantum mechanics, however, is more nonlocal than an LHV model due to having lower uncertainty.[12] The last class of theories, with perfect steering and uncertainty, are much more non-local than quantum mechanics, and lead to the so-called 'non-local box', which, amongst other unphysical properties violates the no-signalling condition.

5.1.1 Comparison and correction of steering inequalities

Returning to our two inequalities 5.1 and 5.3, let us compare their performance in terms of the visibility V and efficiency η, as shown in figure 5.1. There are several important things to note about the figure: first, the optimal choice of measurements for inequality 5.3 are the same as the measurements for 5.1 for $N \in \{2, 3\}$, so performance differences arise solely from the efficacy of the inequalities. Second, the minimum visibility or minimum efficiency is the same for both inequalities, and is known to be optimal for all steering experiments due to fundamental limits[13], however insofar as I am aware it is not known what the tradeoff curve looks like between said endpoints for the optimal steering inequality.

The only complicating factor for the linear inequality is that Alice's measurements must be correlated with Bob's answers—for the quadratic inequality, the sense of Alice's measurements are irrelevant, they need only be correlated *or* anticorrelated with Bob's, while for the linear one she must get the right answer.

Due to the measurements and conditions being identical for both the linear and quadratic steering inequalities, it is a simple matter to reanalyse the data in light of that inequality. Rather than the laborious analysis necessary to correct for the slight non-orthogonality of our measurements given in the paper, for the linear inequality it simply shifts $C_N(\eta)$ up slightly and lifts the degeneracy in Alice's strategy.

It is impossible to perfectly perform a measurement, and indeed is impossible to even determine if you're doing so. One approach to the problem is via detector/process tomography of the

[12] I am not certain if a more-nonlocal theory than classical mechanics exists that doesn't violate no-signalling with zero uncertainty and slightly more steering. I am intrigued by this question, however.

[13] The classical optimal strategy for Alice for lower efficiencies defeats the optimal entangled strategy, for instance.

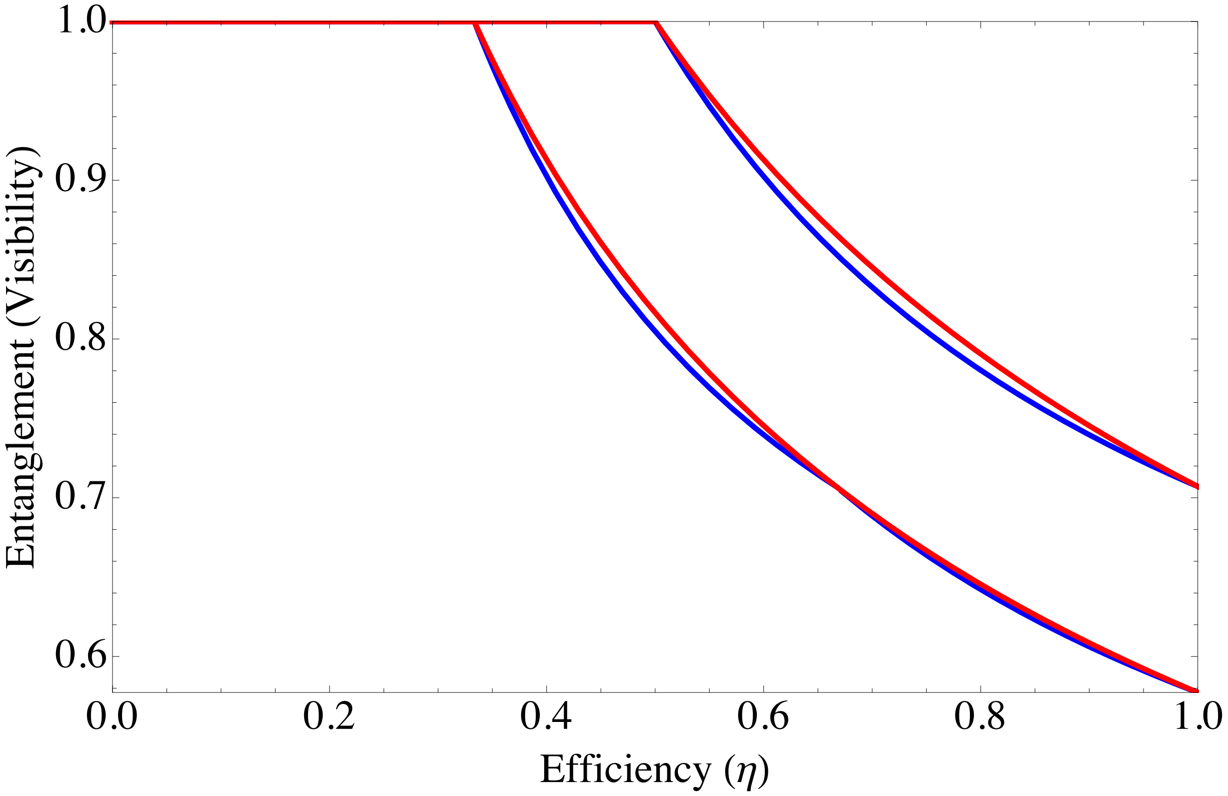

Figure 5.1: A comparison of the efficiency of linear and quadratic steering inequalities. The red curves are the optimal performance curves for a quadratic steering inequality 5.1, whilst the blue is that for the linear inequality 5.3. The upper curves are for $N = 2$ bases, the lower for $N = 3$. For higher N only the linear inequality is possible. At the endpoints the curves meet, as well as at $\eta = 2/3$ for $N = 3$. Figure courtesy C. Branciard.

Table 5.1: The various imperfections of concern for a steering experiment: the efficiency mismatch between the detectors and the orthogonality of the various basis vectors.

Parameter	Value	Uncertainty
η_+/η_-	1.0114	±0.0007
$Y \cdot Z$	0.0083	±0.0010
$Z \cdot X$	0.0134	±0.0007
$X \cdot Y$	0.00013	±0.00015

measurement apparatus, and then using the measurements found through tomography to find the best classical strategy. Wittmann and his colleagues' paper on steering [Wit+12] takes this approach, where they claim that the imperfections in their measurement are sufficient to cover any security hole as the beam-splitter used fails sufficiently often to steer the photon correctly as to add enough random noise. Unfortunately, their paper does not go into sufficient detail for me to be fully confident that they have carefully considered all attacks—that for each pure state strategy of Alice's S_N is less than one, for instance, and worse yet any possible multiphoton strategy.

On the other hand, we considered specific imperfections that are exploitable in the analysis and constructed a worst-case scenario for Bob given his understanding of his measurement apparatus. The two primary security flaws discovered are that his measurements are not perfectly orthogonal, and that the efficiency of his two detectors are not equal.

If Bob's measurement bases are not perfectly orthogonal (on the Bloch sphere) , as shown in figure 5.2 c, then the best separable state strategy's degeneracy lifts: Rather than any superposition of (for two bases) $\{|H\rangle, |V\rangle\}$ and $\{|+\rangle, |-\rangle\}$, the measurement directions that form an acute angle become exploitable. That is, if instead of measuring $|+\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$, Bob measures

$$|\theta\rangle \equiv \cos\theta\,|H\rangle + \sin\theta\,|V\rangle$$

for values of θ slightly less than $\pi/4$, Alice's optimal unentangled input becomes

$$\frac{1}{\sqrt{2}}\left(|H\rangle + |\theta\rangle\right) = \left|\frac{\theta}{2}\right\rangle.$$

Following through the mathematics, this shifts Alice's best-case outcome upwards slightly, independently of the inequality used. For the quadratic inequality, this increases as the inner product of the Bloch sphere vectors. (See appendix C.) For the linear inequality, if $u \cdot v\epsilon$ is the inner product on the Bloch sphere of the two basis vectors and $N = 2$, then rather than $\left\langle A_i \sigma_i^B \right\rangle$ being $\sin(\pi/4) = 1/\sqrt{2}$ it is the slightly higher

$$\sin\left(\frac{\pi}{4} + \frac{\epsilon}{2}\right).$$

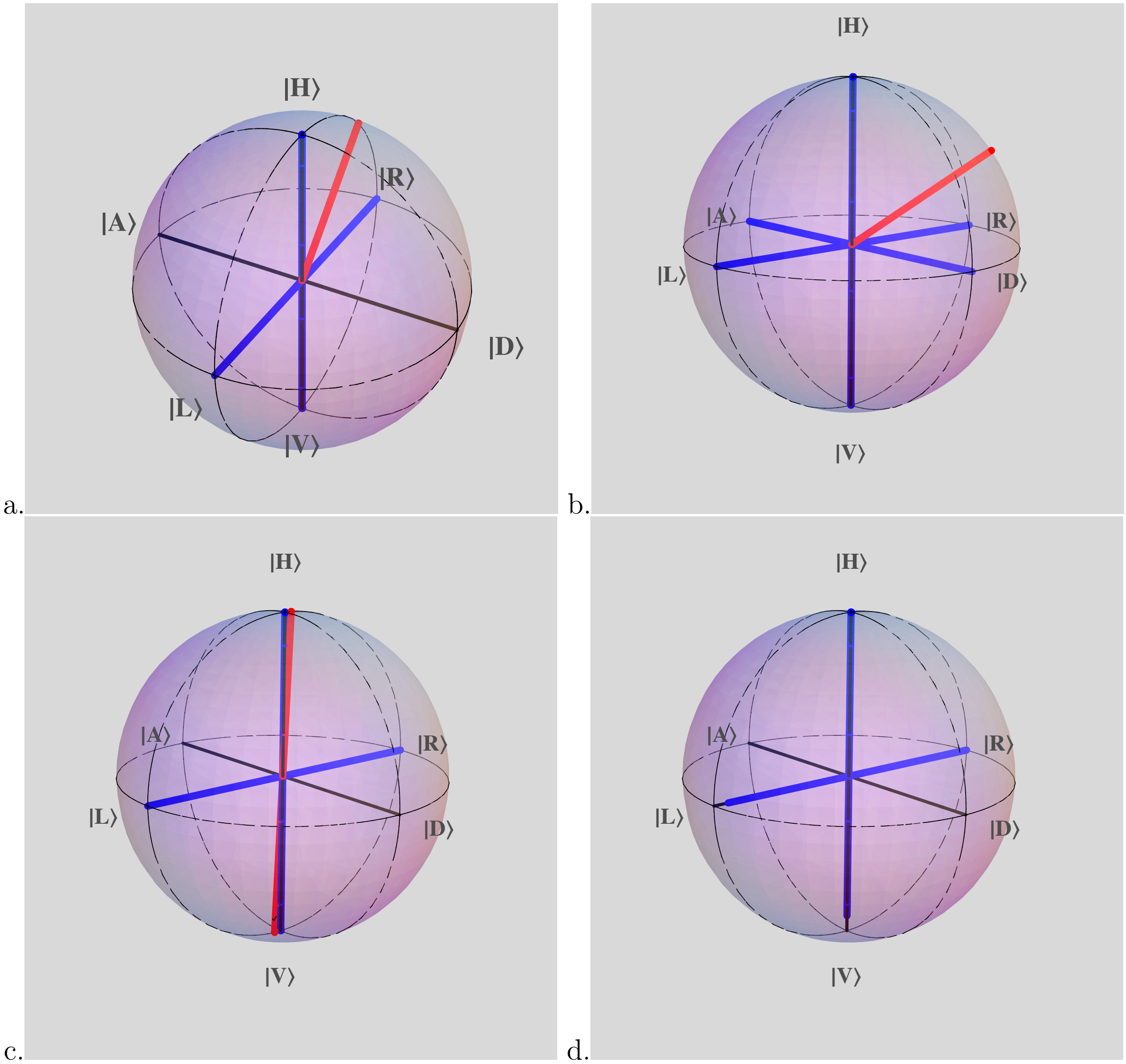

Figure 5.2: a. Alice's optimal unentangled state for a two-basis steering protocol where Bob's measurements are along $|H\rangle$, $|V\rangle$, $|L\rangle$ and $|R\rangle$. By symmetry, the other points equidistant from the basis vectors are also optimal
b. When Bob measures in all three orthogonal bases, Alice's optimal unentangled state remains equidistant from all three.
c. One possible error in Bob's apparatus is if the measurement bases are slightly misaligned. Here his ideal measurement is in blue, while a misaligned measurement is slightly offset in red. This gives Alice a way to exploit him, increasing her possible unentangled outcome.
d. Bob's other possible error is if the efficiency of his detectors are not the same. Here the vectors denoting $|L\rangle$ and $|V\rangle$ are shorter, indicating a lower efficiency. This biases his measurement outcomes towards $|H\rangle$ and $|R\rangle$, again providing Alice with a way to increase the steering parameter.

A further correction arises from a mismatch in the detection efficiencies of the two outputs. Say that η_+, the efficiency of the detector outputting +1 is greater than η_-, the efficiency of the other detector. Then Alice has an obvious strategy: she simply guesses that Bob gets +1 more than -1. In principle this can be solved by inverting the two detectors at some times, but even that can affect the relative coupling efficiency if the inverting element affects the coupling efficiency.

For the linear inequality, rather than a state defined by a Bloch vector b having expectation value $b \cdot u$, it has

$$\left|\left\langle \sim \sigma_i^B \right\rangle\right| \leqslant w[\delta + (1-\delta)\,|b \cdot u|]. \tag{5.8}$$

Here $w \equiv \eta_+/\eta_-$[14], and

$$\delta \equiv \frac{\eta_+ - \eta_-}{2\eta_+} = \frac{1}{2} - \frac{1}{2w}.$$

For a derivation of equation 5.8, see the methods section in appendix C.

Other sources of imperfection in measurements exist, of course: the polarising element will not perfectly polarise the light, background noise will cause random clicks, and so on. However, these all should only be able to reduce the steering parameter, not increase it.

5.2 Results

The raw data from our experiment is presented in table 5.2, while the final data is shown in 5.3. The quadratic results are from Appendix C, while the linear results are freshly analysed for this thesis. All of the results presented are from the same data run, just analysed in light of different inequalities: the choice of which subset of measurements to use for the two-basis case was made to minimise the error in the measurements themselves, *i.e.* the two most orthogonal bases were chosen. Recall that for the linear inequality the the threshold depends on the efficiency of the experiment while for the quadratic one it remains constant for all η.

A surprising outcome to me, at least, is that the violation in terms of standard deviations was greater for quadratic inequality than the linear one. The relative error in the linear steering parameter is higher than for the quadratic steering parameter: this I found surprising, as just by staring at inequalities 5.1 and 5.3 that does not make itself immediately apparent.

Nonetheless, both inequalities are comprehensively violated by the measurements taken, with the smallest violation, by 7 standard deviations, having a failure chance of less than one in a trillion.

[14] I am assuming without loss of generality that $\eta_+ > \eta_-$

Table 5.2: The raw steering experiment results. A_i is Alice's result, while the other column labels are the basis choices. The left column for each basis is $B_i = -1$, and the right is then obviously $B_i = +1$. $A_i = 0$ is a loss event for Alice. Values in the table are single photon counts, taken over 60 s, and suffer from approximately Poissonian error.

A_i	Z		Y		X	
1	1545	221232	4461	232444	4133	228852
0	143364	124951	152535	132001	148427	129528
-1	210094	2083	213456	4907	212603	4555

Table 5.3: A comparison of the violations of the various steering parameters measured and their violation of the relevant inequality. S_N are the quadratic inequality values, while $\mathcal{S}_N$ are the linear inequality values. 'Threshold' the corrected bound, either $C_N(\eta)$ or 1, modified by the vulnerabilities discussed in the text. On the basis of these results linear inequality appears to be more vulnerable to experimental errors, with the relative uncertainty in S_2 being much smaller than that in $\mathcal{S}_2$.

Parameter	Value	Threshold	Violation (std. deviations)
S_3	1.7408±0017	1.062±0.003	>200
S_2	1.1410±0.0014	1.029±0.0019	48
$\mathcal{S}_3$	0.968±0.0004	0.76446±0.00012	90
$\mathcal{S}_2$	0.960±0.002	0.942±0.0003	7

5·3 Squashing

In the paper, we mention near the end 'squashing' as a potential solution to the problem of states of light that are not qubits, and hope that they can be applied to the problem of quantum steering.

'Squashing' arguments solve a problem that's often swept under the rug—that optical modes are *not* just qubits. The assumption is typically made that if you do two-outcome measurements on the modes, such as the polarisation measurements done here, and treat them as qubit measurement outcomes then your protocol, dependent on analysis done on qubits, will succeed.

However, this is not obviously so; it is not difficult to imagine ways in which correlations between the qubit state of interest and additional degrees of freedom could complicate matters. As an example, treatment of the outcome 'both detectors click' is problematic: if Bob simply discards these events then a malicious party can break the protocol. Bob must instead, in such cases, randomly choose a measurement outcome—many early QKD system were not aware of this problem, and thus were subject to a class of attacks.

There is or was some hope, however, as Beaudry, Moroder, *et alii* showed in [BML08; Mor+10] that for a large class of quantum communication protocols including situations analogous to our two-basis measurements that it is the case that you can treat your measurement outcomes as qubit measurements, so long as you follow some precautions as above. The reason that this is true is that there exists a squashing operator that transforms the entire mode Hilbert space into the simple qubit space in a quantum-mechanically legal way.

It seems likely on the surface that a squashing-type argument would be extensible to the case of three orthogonal measurements for steering, though the result in [BML08] that this was not true for the analogous QKD protocol (the six-state protocol) should have been worrisome.

We were hopeful of two things: first, that extensions to larger numbers of bases would be possible, and second that the squashing argument and the correction required due to experimental constraints on the perfection of measurements would be compatible.

The second of those hopes still lives, it remains a conjecture though one that I think is more relevant than theorists give it credit for: Beaudry, Gühne, and Moroder have all given their opinion to me that it should be true, and an interesting thing for a new grad student to work on. It would be nice if that student exists soon.

On the other hand, shortly after we published the paper, it was found that squashing arguments could not hold for greater than two bases in general[15] (for qubit steering inequalities[16]). This has consequences for all steering inequalities, as well as applications thereof. It also means that the steering inequalities discussed above when generalised to large numbers of bases are vulnerable in principle to attack from multiphoton states[17].

As a major consequence, this leaves our $N = 2$ result in the paper as the only definitive steering result at the present time, with the results of Wittmann's, and Bennet's groups [Wit+12; Ben+12] having this security vulnerability. All non-locality results with more than two bases of measurement, and even those with two non-orthogonal bases should be careful to ensure that their results hold in the presence of multiphoton states.

5.4 One-sided device independent QKD

Having reached efficiency values of 72% or so in the lab (in an easier experimental setup), an attempt was made to perform the one-sided device independent QKD protocol described in section 2.1.4. Unlike our steering experiment, we decided it was essential to choose the basis for each measurement at random to properly emulate field conditions for QKD, as a key generated without bit-by-bit randomness of the measurement basis is not, in fact, secure. While

[15] I believe this was in a conference presentation that doesn't seem to appear anywhere. The result has been relayed to me by C. Branciard.

[16] The result is, more precisely, that the full set of measurements must not be overcomplete. This allows some complicated POVM-based QKD protocols that have more than four measurement outcomes.

[17] Assuming of course another argument isn't found to prevent them. Squashing models assume click/no-click detectors, *i.e.* ones that can't resolve photon number, for instance. I am not sure if any work has been done with side-channel attacks on number resolving detectors. I also believe that the squashing no-go theorem isn't constructive.

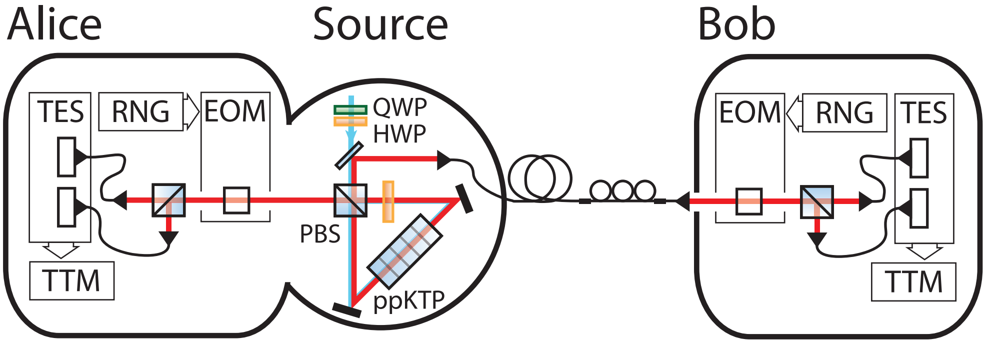

Figure 5.3: A schematic of the setup for this one-sided device independent QKD experiment. The source emits photons to Alice in free space, which she measures using a Pockels cell (EOM) controlled with a random number generator and a polarising beam splitter, then detects the outcome using a set of transition edge sensors. Bob's photon is coupled into a fibre and then emitted into a similar measurement apparatus at a distance from the source: in the actual TES are about .1" (2.5 mm) apart. Bob's apparatus is carefully characterised and trusted, while Alice's needn't be. In practice, Alice's measurement is as carefully set up as possible, of course. Figure courtesy A. Fedrizzi.

a proof-of-principle can be made without basis choice, cryptographers (quantum or otherwise) would not accept such a demonstration as definitive. The alternative method of randomising bases, by using a plain beam-splitter followed by four detectors adds to the experimental complexity of alignment, and also potentially suffers from attacks due to the variance of detector performance.

Therefore, each of the measurement devices used a random number generator[18] and a Pockels cell (or electroöptic modulator (EOM)). A Pockels cell is a birefringent material held between two electrodes across which a variable electric field is available. Via the electroöptical effect, the change in electrical field causes a change in the indices of refraction of the crystal. The cell thus acts as a variable waveplate; typically, they are set up with a fast switch between two voltage levels (zero and some hundreds of volts), and thus can switch between two different measurement bases. The experimental setup can be seen in figure 5.3.

Post-processing of the signals received is also necessary in a QKD system: one must extract from the measurement record the relevant results, and then correct that record to eliminate the inevitable errors therein. To do so a collaboration with the Austrian Institute of Technology was formed to do so carefully and precisely with their QKD 'stack'. This protocol, unlike a typical QKD scheme, requires the efficiency as an input to the privacy amplification step of the protocol but otherwise is very similar: a sift is performed to find errors, followed by a hash of the remaining string to ensure secrecy.

Many months of attempts were insufficient to attain the required efficiency versus visibil-

[18] Either a pseudorandom number generator, or a pregenerated random string; we do not have a relevantly useful true random number generator on hand.

ity tradeoff. Unbeknownst to me before the attempts began our entanglement visibility had dropped significantly while I had been increasing the heralding efficiency of the source, to about 97%. A rebuild failed to solve the problem, while our last-gasp attempt to improve efficiency by changing the fibres connected to the fridge has taken approximately seven times longer than anticipated, and is not yet complete as of the time of this writing.

5.5 Bell tests

The first loss-sensitive Bell inequality was that of Clauser and Horne [CH74] in 1974, which also has the benefit of only requiring one detector on each side:

$$p_{12}(a,b) + p_{12}(a,b') + p_{12}(a',b) - p_{12}(a',b') \leqslant p_1(a) + p_2(b), \tag{5.9}$$

where $p_{12}(\alpha,\beta)$ is the probability of receiving a photon at both detectors when set to settings α and β, while $p_{i\in\{a,b\}}(\cdot)$ is the probability of receiving a photon at detector i[19].

Note that for a continuous source such as the one in use here probabilities are difficult to measure. Fortunately, Eberhard shows that the inequality still holds if one replaces the probabilities with count rates in [Ebe93]; for a simple discussion of that derivation see [Giu+13][20]. Thus, inequality 5.9 becomes

$$C_{12}(a,b) + C_{12}(a,b') + C_{12}(a',b) - C_{12}(a',b') - S_1(a) - S_2(b) \leqslant 0, \tag{5.10}$$

or equivalently

$$\frac{C_{12}(a,b) + C_{12}(a,b') + C_{12}(a',b) - C_{12}(a',b')}{S_1(a) + S_2(b)} \leqslant 1. \tag{5.11}$$

Here C_{12} is the coincidences between the channels, while S is the number of photons arriving at that particular detector for the various settings.

Initially, it was thought that a symmetric heralding efficiency $\eta > 2(\sqrt{2}-1) \approx 82.8\%$ was necessary to violate any loss-sensitive Bell inequality, given a binary, bipartite maximally entangled states such at those use in the steering experiment above, *e.g.*, the singlet state $|01\rangle - |10\rangle$. However that turns out to be the hardest possible case: both increasing the number of degrees of freedom, or reducing the degree of entanglement allow for more loss [Ebe93].

Given states such as $\sin^2(\theta)\,|01\rangle - \cos^2(\theta)\,|10\rangle$,[21] Eberhard pointed out [Ebe93] that, as the

[19] Apologies for the change in notation, this one is typical for the CH inequality

[20] Note that the inequality in this paper to start with appears to be different, though the conclusion is the same. There is a broad equivalency between various Bell-type inequalities.

[21] Also seen parametrized as $(1+r^2)^{-1}(|01\rangle - r\,|10\rangle)$ in the literature. This has an obvious point of maximum entanglement and separability and a direct amount of 'entanglement', while my parameterisation translates easily into state creation angles.

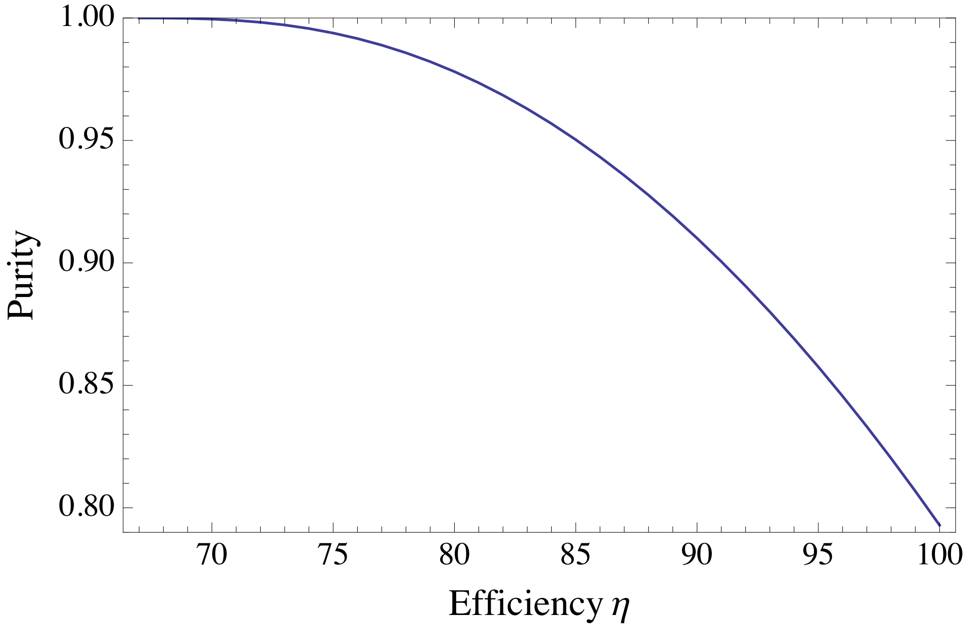

Figure 5.4: The area above the blue curve is the region for which a Bell violation is possible. Note that this figure is concave down, contrasting with figure 5.1. For any given choice of measurments or quantum state this would not be true, but for the convex hull of all choices this is the outcome. This implies that attaining the required state quality to violate the inequality is much more crucial than for a steering inequality, as the tradeoff between efficiency and quality is much more poor. Note that I am using purity for the quality measure here instead of visibility as nonmaximally entangled states are optimal for $\eta < 1$, and have less than perfect visibility in some bases.

state approaches maximal separability (say, as $\theta \to 0$), the required efficiency approaches 2/3. One thing to note here is that for each θ the optimal measurements $\{a, a', b, b'\}$ to violate the inequality also shift—and in an unintuitive way, at least to me. As the degree of entanglement drops the measurement angles shift closer and closer together (while remaining evenly spaced), and shift towards the *less* likely measurement outcome. For instance, as the state approaches $|HV\rangle$, the measurement angles for Alice approach V, while those for Bob approach H.

However, as the amount of entanglement in the state drops, the required visibility rises due to the measurements approaching each other. Thus, for optimal $\{\theta, a, a', b, b'\}$ the quality versus efficiency curve is concave down, rather than up as it is in our work on steering (see figure 5.4). For any given choice of θ the graph is concave up, but the convex hull of all such values is, as shown, concave up. Thus, for a Bell inequality the tradeoff between inefficiency and infidelity[22] in the state is a much harder relation.

This differing nature of this tradeoff also puts more stringent requirements on the measurement device itself—for small θ light that must nearly all be rejected is shone upon the device, amplifying any errors therein. I tried several measurement devices in my pursuit of a Bell

[22] Or invisibility?

violation:

A simple plate polariser The extinction of the polariser turned out to be insufficient, transmitting too much light that should be rejected, while the performance in transmission was actually fine.

A calcite beam displacer mounted on a rotation stage. The thickness of a beam displacer—in this case 25 mm—amplified the small errors in the end facets of the device. As the device was rotated the output beam wandered sufficiently to ruin the experiment.

A waveplate followed by a calcite beam displacer. This was the most successful alternative, and indeed was the one used in [Giu+13] to close the detection loophole. The added surfaces, each causing loss, were problematic for me, as well as a concern over the effective extinction ratio due to large beam diameter. However, of the three alternatives this one showed the most promise.

I attempted to violate a Bell inequality when our efficiency was about 73%[23], however our state visibility was insufficient to violate the inequality. Unfortunately, after rebuilding the source to attempt to increase the state quality (by angling the PBS away from normal incidence) all attempts to regain the necessary efficiency have failed,[24] and the decision was made to defer this experiment until the conclusion of the quantum key distribution experiment, above.

[23] In practice the efficiency of the clockwise pumping direction and the counterclockwise pumping direction is not the same. For this experiment you would, per Cyril Branciard in a private communication, like to align the efficient direction with the direction of the measurements, not the direction of the majority of the state. As you throw away the majority of the light produced, this actually results in the highest net efficiency.

[24] This is, of course, incredibly frustrating. . . .

Chapter 6

Epilogue

With that, we come to the end of the story, wherein traditionally the disparate threads are brought together, and suggestions of future work are put forward.

Fortunately, the next few experiments for this system are obvious, as shown in the previous chapter: the one-sided device-independent QKD experiment should hopefully be within reach with our upgraded fibre optics installed. The closure of the detection loophole for a Bell test has already been done by others [Giu+13; Chr+13], and I anticipate that both of those efforts will next focus on the simultaneous closure of the locality and detection loopholes. Thus, that effort is not so much 'future work' as 'work-in-progress'.

Beyond that, experiments involving more than two photons are the next step: demonstrating teleportation[1], fusion gates[2], or Knill gates[3] that require four photons and, if sufficiently efficient, can be used for scalable quantum computing.

However, to do so will require a scalable source of photons. The approach presented here—to use a spontaneous process to generate the photons—does not scale well to larger numbers of photons due to the fundamentally random nature of the process. A more reliable approach is necessary. Fortunately, and surprisingly, progress on that front is being made quickly, and our laboratory has begun a collaboration that will bring an example of such a device into operation in our lab. This will allow a few key experiments or developments to occur: the testing of optical quantum gates with true single photons; the development of four-photon processes with much better statistics and fidelities; and the creation of cluster states with reasonable probability. While such sources still have some problems over and above the problem of 'making

[1] The nonlocal transport of quantum information using entanglement and cleverness

[2] A way to staple entangled states together, growing them, at the cost of some of each state. A sufficiently large entangled state of particular kinds 'is' a quantum computer, so getting the fusion yield up is one approach to optical quantum commuting [VBR08]

[3] The other approach to optical quantum computing, using measurement-induced interactions between photons, that requires ancillary photons to avoid loss of information. This approach was pioneered by Knill, Laflamme, and Milburn and is in principle also scalable[KLM01].

photons'—the time-bandwidth product of the photons so produced tends to not be transform limited, for instance—the challenges they present the quantum computer engineer in integrating them into a complete system are different than a parametric down-converter, and ones that will need to be solved before the optical quantum computer is viable.

While the initial studies with a true single photon source can be made with an arbitrary set of detectors this is not true for truly scalable protocols. Indeed, even for relatively small experiments, with four, six, or eight photons, the improvements in statistics, or contrariwise the amount of time the experiment takes, is exponentially related to the efficiency of the detectors. I would thus like to see efforts made to bring our transition edge sensors and our true single photon source brought into the same experiment sooner rather than later. This also, to some extent, solves a few technical issues with the true single photon source's integrability, as the acceptance bandwidth of a TES is much larger than a semiconductor-based detector.

So: Things to do with TES in the context of single photon quantum computing abound, but will all require a step above where we are now. Rather than using two or four detectors and two photons, the next tier of interesting experiments requires four-eight detectors and four photons.

I hope that I have brought new information to you, the reader, on the difficulties and reasons for integrating disparate technologies together, and thrown some light on the possible utility of doing so.

Farewell.

Bibliography

[ADR82] A. Aspect, J. Dalibard, and G. Roger. "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers". In: *Phys. Rev. Lett.* 49 (25 1982), pp. 1804–1807. DOI: 10.1103/PhysRevLett.49.1804. URL: http://link.aps.org/doi/10.1103/PhysRevLett.49.1804.

[AGR81] A. Aspect, P. Grangier, and G. Roger. "Experimental Tests of Realistic Local Theories via Bell's Theorem". In: *Phys. Rev. Lett.* 47 (7 1981), pp. 460–463. DOI: 10.1103/PhysRevLett.47.460. URL: http://link.aps.org/doi/10.1103/PhysRevLett.47.460.

[AGR82] A. Aspect, P. Grangier, and G. Roger. "Experimental Realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A New Violation of Bell's Inequalities". In: *Phys. Rev. Lett.* 49 (2 1982), pp. 91–94. DOI: 10.1103/PhysRevLett.49.91. URL: http://link.aps.org/doi/10.1103/PhysRevLett.49.91.

[BB84] C. H. Bennett and G. Brassard. *Advances in Cryptology: Proceedings of Crypto'84*. 1984.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. "Quantum cryptography without Bell's theorem". In: *Phys. Rev. Lett.* 68 (5 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557. URL: http://link.aps.org/doi/10.1103/PhysRevLett.68.557.

[Bel64] J. S. Bell. "On the Einstein Podolsky Rosen Paradox". In: *Physics* 1 (1964), pp. 195–200.

[Ben10] R. Bennink. "Optimal Co-linear Gaussian Beams for Spontaneous Parametric Down-Conversion". In: *Phys. Rev. A* 81 (2010), p. 053805.

[Ben+12] A. Bennet et al. "Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loopholes". In: *Physical Review X* 2 (2012), p. 031003.

[BML08] N. J. Beaudry, T. Moroder, and N. Lütkenhaus. “Squashing Models for Optical Measurements in Quantum Communication”. In: *Phys. Rev. Lett.* 101 (9 2008), p. 093601. DOI: `10.1103/PhysRevLett.101.093601`. URL: `http://link.aps.org/doi/10.1103/PhysRevLett.101.093601`.

[Bra+09] A. M. Braǹcyzk et al. “Optimised generation of heralded Fock states using parametric down conversion”. In: *arxiv:0909.4147v2 [quant-ph]* (2009).

[Bra+12] C. Branciard et al. “One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering”. In: *Phys. Rev. A* 85 (1 2012), p. 010301. DOI: `10.1103/PhysRevA.85.010301`. URL: `http://link.aps.org/doi/10.1103/PhysRevA.85.010301`.

[CH74] J. F. Clauser and M. A. Horne. “Experimental consequences of objective local theories”. In: *Phys. Rev. D* 10 (1974), p. 526.

[Chr+13] B. G. Christensen et al. “Detection-Loophole-Free Test of Quantum Nonlocality, and Applications”. arXiv:1306.5772 [quant-ph]. 2013.

[DiV00] D. P. DiVincenzo. “The Physical Implementation of Quantum Computation”. In: *Fortschritte der Physik* 48 (2000), p. 771.

[Dou+10] A. Dousse et al. “Ultrabright source of entangled photon pairs”. In: *Nature* 466 (2010), pp. 217–220.

[Ebe93] P. H. Eberhard. “Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment”. In: *Phys. Rev. A* 47 (2 1993), R747–R750. DOI: `10.1103/PhysRevA.47.R747`. URL: `http://link.aps.org/doi/10.1103/PhysRevA.47.R747`.

[Eis+11] M. D. Eisaman et al. “Invited Review Article: Single-photon sources and detectors”. In: *Review of Scientific Instruments* 82.7, 071101 (2011), pp. –. DOI: `http://dx.doi.org/10.1063/1.3610677`. URL: `http://scitation.aip.org/content/aip/journal/rsi/82/7/10.1063/1.3610677`.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. “Can Quantum-Mechanical description of reality be considered complete?” In: *Phys. Rev.* 47 (1935), pp. 777–780.

[F+̀94] J. P. Fève et al. “Repitition rate dependence of grey-tracking in KTiOPO$_4$ during second harmonic generation at 532nm”. In: *Applied Physics Letters* 70.3 (Jan. 1994), pp. 277–279.

[Fio+04] M. Fiorentino et al. “Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints”. In: *Phys. Rev. A* 69.4 (2004), p. 041801. DOI: `10.1103/PhysRevA.69.041801`.

[Fuk+11] D. Fukuda et al. "Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling". In: *Optics express* 19.2 (2011), pp. 870–875.

[Gaz+13] O. Gazzano et al. "Entangling Quantum-Logic Gate Operated with an Ultrabright Semiconductor Single-Photon Source". In: *Phys. Rev. Lett.* 110 (25 2013), p. 250501. DOI: 10.1103/PhysRevLett.110.250501. URL: http://link.aps.org/doi/10.1103/PhysRevLett.110.250501.

[Ger+11] T. Gerrits et al. "On-chip, photon-number-resolving, telecommunication-band detectors for scalable photonic information processing". In: *Phys. Rev. A* 84 (6 2011), p. 060301. DOI: 10.1103/PhysRevA.84.060301. URL: http://link.aps.org/doi/10.1103/PhysRevA.84.060301.

[Ger+12] T. Gerrits et al. "Joint Spectral Measurements at the Hong-Ou-Mandel Interference Dip". In: *11th Intl. Conference on Quantum Communication, Measurement and Computing.* 2012.

[Giu+13] M. Giustina et al. "Bell violation using entangled photons without the fair-sampling assumption". In: *Nature* 497 (2013), pp. 227–230. DOI: 10.1038/nature12012.

[Hal+07] M. Halder et al. "Entangling independent photons by time measurement". In: *Nature Physics* 3 (2007), p. 692. URL: doi:10.1038/nphys700.

[Ham] Hamamatsu Corp. *Datasheet for PMTs.* URL: http://www.hamamatsu.com/resources/pdf/etd/PMTmodules_TPMO0010E02.pdf.

[HM86] C. Hong and L. Mandel. "Experimental realization of a localized one-photon state". In: *Physical Review Letters* 56 (1986), pp. 58–60.

[Hor+09] R. Horodecki et al. "Quantum Entanglement". In: *Rev. Mod. Phys* 81 (2009). arXiv:quant-ph/0702225v2, pp. 865–942.

[IDQ] IDQuantique. *QKD Products page.* URL: http://www.idquantique.com/network-encryption/technology/qkd.html.

[JBW11] T. Jennewein, M. Barbieri, and A. G. White. "Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis". In: *Journal of Modern Optics* 58.3-4 (2011), pp. 276–287. DOI: 10.1080/09500340.2010.546894. eprint: http://dx.doi.org/10.1080/09500340.2010.546894. URL: http://dx.doi.org/10.1080/09500340.2010.546894.

[JHS93] G. Jaeger, M. A. Horne, and A. Shimony. "Complementarity of one-particle and two-particle interference". In: *Phys. Rev. A* 48 (2 1993), pp. 1023–1027. DOI: 10.1103/PhysRevA.48.1023. URL: http://link.aps.org/doi/10.1103/PhysRevA.48.1023.

[JPK04] E. Jeffrey, N. A. Peters, and P. G. Kwiat. “Towards a periodic deterministic source of arbitrary single-photon states”. In: *New Journal of Physics* 6.1 (2004), p. 100.

[JSV95] G. Jaeger, A. Shimony, and L. Vaidman. “Two interferometric complementarities”. In: *Phys. Rev. A* 51 (1 1995), pp. 54–67. DOI: 10.1103/PhysRevA.51.54. URL: http://link.aps.org/doi/10.1103/PhysRevA.51.54.

[KFW06] T. Kim, M. Fiorentino, and F. N. C. Wong. “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer”. In: *Phys. Rev. A* 73 (2006), p. 012316.

[Kil+10] N. Killoran et al. “Derivation and experimental test of fidelity benchmarks for remote preparation of arbitrary qubit states”. In: *Phys. Rev. A* 81 (1 2010), p. 012334. DOI: 10.1103/PhysRevA.81.012334. URL: http://link.aps.org/doi/10.1103/PhysRevA.81.012334.

[Kim+09] Y.-S. Kim et al. “Silicon Single-Photon Detector with 5 Hz Dark Counts”. In: *Conference on Lasers and Electro-Optics.* Optical Society of America. 2009, JThE103.

[KLM01] E. Knill, R. Laflamme, and G. Milburn. “A scheme for efficient quantum computation with linear optics”. In: *Nature* 409.6816 (2001), p. 46.

[Kuk+04] C. E. Kuklewicz et al. “High-flux source of polarization-entangled photons from a periodically poled KTiOPO$_4$ parametric down-converter”. In: *Phys. Rev. A* 69.1 (2004), p. 013807. DOI: 10.1103/PhysRevA.69.013807.

[Kwi+95] P. Kwiat et al. “New High-Intensity Source of Polarization-Entangled Photon Pairs”. In: *Phys. Rev. Lett.* 75.24 (1995), pp. 4337–4342.

[LL+13] A. Lamas-Linares et al. “Nanosecond-scale timing jitter in transition edge sensors at telecom and visible wavelengths”. In: *Applied Physics Letters* 102 (2013), p. 231117.

[LMN08] A. E. Lita, A. J. Miller, and S. W. Nam. “Counting near-infrared single-photons with 95% efficiency”. In: *Opt. Express* 16.5 (2008), pp. 3032–3040. DOI: 10.1364/OE.16.003032. URL: http://www.opticsexpress.org/abstract.cfm?URI=oe-16-5-3032.

[LT05] D. Ljunggren and M. Tenger. “Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers”. In: *Phys. Rev. A* 72 (2005), p. 062301.

[Lun+09] J. S. Lundeen et al. “Measuring measurement”. In: *Nature Physics* 5 (2009), p. 27.

[Mag] MagiQ Technologies. *QBox Datasheet.* URL: http://www.magiqtech.com/MagiQ/Products_files/QBoxDatasheet-2011.pdf.

[Mat+09] J. C. Matthews et al. “Manipulation of multiphoton entanglement in waveguide quantum circuits”. In: *Nature Photonics* 3.6 (2009), pp. 346–350.

[MG25] A. A. Michelson and H. G. Gale. “The Effect of the Earth’s rotation on the velocity of light”. In: *The Astrophysical Journal* 61 (1925), pp. 140–145.

[Mik+08] S. Miki et al. “Large sensitive-area NbN nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates”. In: *Applied Physics Letters* 92.6 (2008), pp. 061116–061116.

[Mit09] M. W. Mitchell. “Parametric down-conversion from a wave-equation approach: Geometry and absolute brightness”. In: *Phys. Rev. A* 79 (4 2009), p. 043835. DOI: `10.1103/PhysRevA.79.043835`. URL: `http://link.aps.org/doi/10.1103/PhysRevA.79.043835`.

[Mor+10] T. Moroder et al. “Entanglement verification with realistic measurement devices via squashing operations”. In: *Phys. Rev. A* 81.5 (2010). See the proof of Theorem V.1. in particular., p. 052342. DOI: `10.1103/PhysRevA.81.052342`.

[Mun+08] W. J. Munro et al. “High-Bandwidth Hybrid Quantum Repeater”. In: *Phys. Rev. Lett.* 101 (4 2008), p. 040502. DOI: `10.1103/PhysRevLett.101.040502`. URL: `http://link.aps.org/doi/10.1103/PhysRevLett.101.040502`.

[Nau+13] S. Nauerth et al. “Air-to-ground quantum communication”. In: *Nature Photonics* 7.5 (May 2013), pp. 382–386.

[Ou07] Z.-Y. J. Ou. *Multi-Photon Quantum Interference*. New York: Springer, 2007.

[OW10] J. Oppenheim and S. Wehner. “The Uncertainty Principle Determines the Nonlocality of Quantum Mechanics”. In: *Science* 330.6007 (2010), pp. 1072–1074. DOI: `10.1126/science.1192065`. eprint: `http://www.sciencemag.org/content/330/6007/1072.full.pdf`. URL: `http://www.sciencemag.org/content/330/6007/1072.abstract`.

[PMO09] A. Politi, J. C. Matthews, and J. L. O’Brien. “Shor’s quantum factoring algorithm on a photonic chip”. In: *Science* 325.5945 (2009), pp. 1221–1221.

[Pri] Princton Lightwave. *PGA-200 Cooled Single Photon Counting Avalanche Photodiode - Discrete*. URL: `http://www.princetonlightwave.com/mm-products/single-photon-detectors/gmapds/pga-200-cooled-single-photon-counting-avalanche-photodiode-discrete#specifications`.

[Ram+12] S. Ramelow et al. “Highly efficiency heralding of engangled single photons”. arXiv:1211.5059. 2012.

[Rec+94] M. Reck et al. “Experimental realization of any discrete unitary operator”. In: *Phys. Rev. Lett.* 73 (1 1994), pp. 58–61. DOI: `10.1103/PhysRevLett.73.58`. URL: `http://link.aps.org/doi/10.1103/PhysRevLett.73.58`.

[Red05] S. Redner. “Citation Statistics from 110 Years of Physical Review”. In: *Physics Today* 58 (2005), p. 49.

[Sag13] G. Sagnac. “L’éther lumineux démontré par l’effet du vent relatif d’éther dans un interféromètre en rotation uniforme”. In: *Comptes Rendus* 157 (1913), pp. 708–710.

[San+01] C. Santori et al. “Triggered single photons from a quantum dot”. In: *Physical Review Letters* 86.8 (2001), p. 1502.

[Sau+10] D. J. Saunders et al. “Experimental EPR-steering using Bell-local states”. In: *Nature Physics* 6.11 (Nov. 2010), pp. 845–849.

[Say+11] C. Sayrin et al. “Real-time quantum feedback prepares and stabilizes photon number states”. In: *Nature* 477.7362 (2011), pp. 73–77.

[Sch35] E. Schrödinger. “Die gegenwärtige Situation in der Quantenmechanik”. In: *Die Naturwissenschaften* 23 (1935). In german, pp. 807–812; 823–828; 844–849.

[Shi07] A. J. Shields. “Semiconductor quantum light sources”. In: *Nature photonics* 1.4 (2007), pp. 215–223.

[Sho95] P. W. Shor. “Scheme for reducing decoherence in quantum computer memory”. In: *Phys. Rev. A* 52 (4 1995), R2493–R2496. DOI: `10.1103/PhysRevA.52.R2493`. URL: `http://link.aps.org/doi/10.1103/PhysRevA.52.R2493`.

[Smi09] D. H. Smith. “An ultrafast source of polarization entangled photon pairs based on a Sagnac interferometer”. MA thesis. University of Waterloo, 2009.

[Smi+12] D. H. Smith et al. “Conclusive quantum steering using superconducting transition-edge sensors”. In: *Nature Communications* 3 (2012), p. 625. DOI: `10.1038/ncomms1628`.

[Stu+09] D Stucki et al. “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres”. In: *New Journal of Physics* 11.7 (2009), p. 075003. URL: `http://stacks.iop.org/1367-2630/11/i=7/a=075003`.

[SW00] J. H. Shapiro and N. C. Wong. “An ultrabright narrowband source of polarization-entangled photon pairs”. In: *Journal of Optics B: Quantum and Semiclassical Optics* 2 (Feb. 2000), pp. L1–L4.

[Tan+01] S. Tanzilli et al. “Highly efficient photon-pair source using periodically poled lithium niobate waveguide”. In: *Electronics Letters* 37.1 (2001), pp. 26–28.

[VBR08] M. Varnava, D. E. Browne, and T. Rudolph. “How good must single photon sources and detectors be for efficiently linear optical quantum computation?” In: *Phys. Rev. Lett.* 100 (2008), p. 060502.

[Wei+98] G. Weihs et al. “Violation of Bell’s Inequality under Strict Einstein Locality Conditions”. In: *Phys. Rev. Lett.* 81.24 (1998), pp. 5039–5043.

[Wit+12] B. Wittmann et al. “Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering”. In: *New Journal of Physics* 14.5 (2012), p. 053030.

[WJD07] H. M. Wiseman, S. J. Jones, and A. C. Doherty. “Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox”. In: *Physical Review Letters* 98.14 (Apr. 2007). URL: `http://link.aps.org/doi/10.1103/PhysRevLett.98.140402`.

[Żuk02] M. Żukowski. *Physics of quantum information. Sketches.* Lecture notes. These appear not to be available on the web, but are in reasonably wide circulation. Contact me for a copy if neccessary. 2002.

Appendix A

How to build your own Sagnac source

If one is building a Sagnac source, one first must take into account what one is building it *for*. Theoretical analyses—combined with some experimental exploration of the same parameter space—show that the optima for brightness, asymmetric heralding efficiency, and symmetric heralding efficiency are not coincident. So, first things first, decide what you're optimising for and look up the relevant waist diameters to choose some lenses.

As a general piece of advice the following two things are true: first, keep everything as compact as possible, particularly the interferometric loop; and second, minimise the number of lenses in the system. One lens per coupler is sufficient. This has the unfortunate side effect of coupling waist size to waist position, but on the whole has been beneficial.

A.1 Sagnac parts list (minimum):

3 Fibre couplers. Two need to be quite nice, with good repeatability and low cross-coupling, the third, for the pump, is less critical.

3 Lenses. Moulded aspheric lenses work quite well if a suitable focal length is available.

Downconversion crystal and mount. PPKTP[1] is traditional, and has to be temperature controlled. The length of this crystal partially determines your focal parameters, so has to be known first. A roll-pitch-yaw mount is helpful but not critical. Z translation (in the direction of the beam) is also useful.

2 Mirrors. Polarisation insensitive. For the interferometer loop. Note that a rectangular interferometer is a bad idea due to symmetry considerations.

[1] Periodically poled potassium titanic phosphate. Raicol, in Israel, is a good supplier.

Pump half-wave plate(s). A half-wave plate to set the relative amount of H and V polarisation is critical, but need not be particularly accurate. A wave plate set up to change the phase of H vs. V is helpful but can be substituted by a number of other things elsewhere in the setup.

Dual wavelength half-wave plate. This needs to be as accurate as possible for the output wavelength, and small enough to fit in the setup. The one used here was 1/2" diameter. A rotation stage is helpful for alignment but not necessary in principle.

Dichroic mirror. This should separate the input and output wavelengths with a minimum of loss of the output, which typically means it reflects the output wavelength. These are typically custom parts, and made for an AOI of 45°.

Polarising beam-splitter and mount. Should be as highly specced as possible for the output wavelength, and, given that constraint, still work for the pump. This typically means a custom part is necessary. A simple post is sufficient for mounting this device, but a rotation or roll-tip-yaw stage is helpful, especially if optimising the angle of incidence (see below), but is unfortunately larger, making the whole interferometer bigger.

Filters Due to the collinear geometry of a Sagnac source fairly significant filtration of the pump from the output is necessary. A bandpass filter at the centre wavelength of the source, backed with a piece of coloured glass is sufficient. I typically co-mount the filters with the lenses for the coupler, but this is up to the individual experimenter.

Pump laser Typically fibre-coupled, though free-space is fine. For most applications in free space a GaN diode around 405 nm should do the trick, though the Quantum Technology lab works at 410 nm for legacy reasons.

Sheet polariser A simple sheet polariser–or polaroid–is useful to have on hand to look at interference fringes.

A.2 Step-by-step alignment instructions

This is my step-by-step procedure for aligning a Sagnac source; I don't claim it is optimal but I will claim that it works quite well. I have been building and aligning these sources for about seven years now, and this is the best procedure I have come up with.

1. Lay out the entire setup on the bench, ensuring that there is enough space for everything. In particular, make sure you can get to the knobs on everything, particularly the mirrors in the Sagnac loop and on the output fibre couplers. I recommend marking the table with the locations of the critical components.

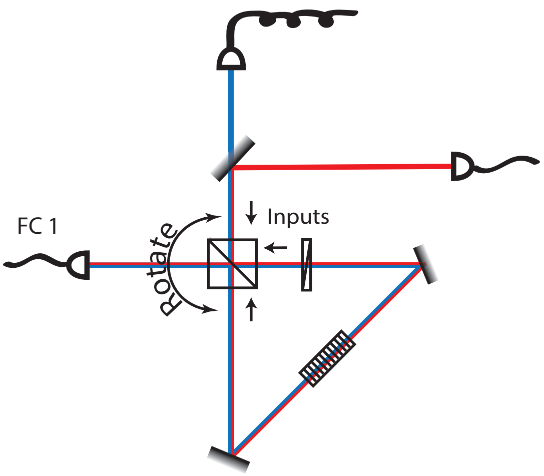

Figure A.1: When optimising the angle of incidence for the PBS, rotate it about the vertical axis while checking the rejection ratio. This is slightly tricky as your meter's sensitivity may depend on the angle of incidence as well. The three inputs shown are the critical ones: no light enters from the left, and the top (pump) input is less important than the two for the signal. Unfortunately, most cube PBS perform better from one side or the other.

2. Remove everything except for the pump and its control optics, as well as the dichroic mirror.

3. Ensure that the dichroic mirror is at the desired angle–this is usually at 45°angle of incidence (AOI), but if space requirements or the coating on the mirror require a different angle, ensure you have it correct. This step is this early because the through-mirror path, usually taken by the pump beam, is steered by passing through the mirror and we'd like to not shift it later.

4. (Optional) If ultimate performance is required, optimise the angle of incidence for the PBS in the Sagnac loop. Shine polarised light of the wavelength of down-conversion light (the "signal" or "idler" wavelength) on the PBS and rotate it until the rejection is optimised. Check the other three input ports of the PBS, and find the best compromise angle for *three* of the inputs—if one is very different make sure it is the output only port (see figure A.1). Set the PBS to have this input angle of incidence—for our device this was at an AOI of about 3°from normal.

   Otherwise, install the PBS at normal incidence to the pump.

5. If you have a beam profiler or other such device, use it to set the pump's focus.

6. Align the Sagnac interferometer to its fringes:

(a) Install the two Sagnac loop mirrors. Insofar as possible, ensure that they are equidistant from the PBS.

(b) Set the pump polarisation to ±45°.

(c) Rough align the two mirrors such that the two counter-propagating beams appear to reflect from the same point on each mirror. You may need to do this under low-light conditions if your mirrors are low-loss.

(d) Use a sheet polariser set to 45° in the output of the interferometer to view the interference fringes on a screen. I find it helpful to reflect the output onto the screen to reduce viewing distance while still allowing the beam to grow to a helpful size.

(e) Walk[2] the two mirrors against each other to find the centre of the interference pattern–either a bright spot or a dark spot. The fringes should get larger than the spot size near the centre of the pattern, making this a challenge.

(f) Once you think you have found the centre of the pattern, rotate the pump polarisation or the sheet polariser to −45°. This should invert the interference pattern, allowing you to check if the pattern is centred. It's rarely perfect on the first try. Iterate on both fringe patterns until you are satisfied that there is perfect overlap between the pumping directions.

(g) Adjust the pump's focus until it is centred in the loop. This can be fairly rough—we'll fix it later. Make sure nothing has happened to your interference fringes.

7. Insert the down-conversion crystal into the loop and back-align[3] it. Make sure that the crystal is in the centre of the loop to within a millimetre or so: this is more critical if your couplers are strongly focussed. If you can't back-align both facets simultaneously then your crystal's end facets aren't parallel. This is a Very Bad Thing. In principle, you can solve this problem[4]. In practice, I don't want to try.

   Make sure you know which way around the crystal axes are. You would like the pump polarisations output by the loop PBS to be parallel and perpendicular to the input polarisation of the crystal. If you have the roll degree of freedom on your crystal's mount try to optimise it, otherwise try to make sure that all your mounts are parallel to the table.

[2] To "walk" two degrees of freedom against each other is to make small consistent permutations in one of them, and then optimise the other. If the new position is better, continue making permutations of the same sign, otherwise go the other way. Ultimately, this should lead to the global optimum over those degrees of freedom, assuming some reasonable things. A lot of this will need to be done.

[3] To "back-align" an optic, look at the reflection from its facet, and adjust the optic until the reflection is directly along the input laser. Use a pinhole—usually punched in a business card—to view this reflection while still allowing light to strike the optic. When doing this in a Sagnac loop you can look at both facets as there is a beam travelling in both directions.

[4] The problem is diffraction at the surfaces: this can be compensated by turning the mirrors slightly. Exactly how much turning given the difference in the index of refraction between the three beams is up to you.

8. Insert the loop HWP into the loop and back-align it. You want it in between the PBS and the crystal in the direction that the pump is perpendicular to the desired pumping direction. Typically this is in the reflected arm, but if your crystal is rotated 90°, such that it should be pumped with horizontally polarised light, then the HWP has to go on the other side.

9. If your output fibre couplers are all-in-one, set them to be as zeroed as possible, such that a beam coupled into or out of the fibre passes through the middle of the collimating lens. It's easiest to do this with two pinholes with a metre or two between them, one of which is directly in front of the coupler. Set the coupler and the pinholes up along a line of an optical table, taking care to make sure the coupler is square to the lines, then shine an alignment beam out of the coupler and pass it through the pinholes.

   If your couplers are in multiple pieces, with the lens and fibre mounted on different stages, skip this step. Instead, be very careful while doing the next step.

10. Place fibre coupler one (see figure 3.1), without any filters. If your central PBS is at normal incidence, make sure the coupler is square with the table. Otherwise, very carefully back align the coupler using the pump beam's reflection from the collimating lens[5]. If your coupler is in two pieces, place the fibre first, then the lens; shine a beam out of the bare fibre to align that piece first, or if you can just mount something on the fibre-tip's stage to back-align with.

11. Check your alignment by shining an alignment laser through the coupler toward the Sagnac; if the angle is way off go back to the previous step. Use the back-alignment from the lens and minor tweaks of the overall position to get things as close as possible to antiparallel. If your alignment laser is close in wavelength to the downconversion wavelength, also roughly set the focus of the coupler here.

12. Couple the pump beam into the coupler; check your coupling with a power meter. Do *not* adjust the focus when optimising the coupling: the optimal focus for the pump and signal wavelengths are sufficiently different as to be useless.

13. Turn the loop HWP to minimise the output from the interferometer—a full characteristisation scan can be done if your mount is repeatable. Due to space limitations, however, this mount is often less than precise, so just do your best.

14. Insert whatever filter you plan on using into this output. If it has tip-tilt degrees of freedom, make sure it's properly aligned; if you're changing the wavelength of an interference

[5] When back-aligning lenses the front- and back-surface reflections should be distinct. This allows you to align both the tip-tilt and centring (x-y) of the lens. When aligned, the two reflections should both be centred on the input beam.

filter by angle tuning do so carefully[6].

15. Plug your output coupler into whatever single photon detector you plan on using. Ideally do this without changing the fibre attached at the coupler, as attaching and removing fibres can cause the coupler to move, as well as being not-quite perfectly repeatable; in particular the cores of different fibres might not be identically located with respect to the connector.

16. Turn on your single photon detector; hopefully you have some counts. If you are uncertain of the operating temperature of your crystal, scan the temperature through the range expected and optimise the count rate[7].

17. If you still have no photons, go back to step 10 and try again[8].

18. Optimise the number of counts at your single photon detector by walking the various degrees of freedom. If you have access to a reasonably efficient in-fibre beam splitter or number resolving detectors, see subsection A.3. You may find that the distribution of singles has two peaks: this is from the clockwise and counterclockwise beam paths being imperfectly overlapped, and implies you didn't get the interferometer or crystal perfectly aligned earlier. For now, find the best compromise position.

19. Place fibre coupler two (see figure 3.1). Rough align it in the same way that coupler one was aligned; every dichroic mirror I have used in a Sagnac-type source has been sufficiently lossy to allow alignment to the pump. Be careful, however, to align to the correct reflection from the dichroic: on many carelessly made dichroic mirrors the other surface is uncoated and reflects more of the pump than the 'mirrored' side.

20. If you have a laser that passes through the filter in coupler #1, optimise the alignment of coupler #2 by coupling the light from one coupler into the other: I have tried this both coupling from #1 to #2 and vice versa, to no apparent effect.

    - Ensure that the loop HWP is set to allow light to pass through the interferometer

[6] The centre wavelength of an interference filter can be reduced by tipping the filter with respect to the beam. $\lambda(\theta) \approx \lambda_0 \sin^2(\theta)$, for angle of incidence θ.

[7] A couple of options for temperature tuning present themselves. If you have a broad filter available in addition to whatever you plan on ultimately using, you can align the source with just that filter present, then switch in the narrower filter if desired or necessary and temperature tune the crystal then. If you have a spectrometer or wavemeter with single photon sensitivity, feel free to just use it to find out the output spectrum. Finally, if you're going to interfere the outputs from the source you can use the resulting Hong-Ou-Mandel interference visibility to tune the temperature of the crystal to produce degenerate outputs.

[8] Alternatively, just start turning knobs and hoping for the best. This rarely works but often makes experimentalists feel better.

- Try to ensure that the polarisation being used for this alignment is approximately even proportions of horizontal and vertical: just bend the input fibre until this is the case.
- Feel free to adjust the focus of coupler #2 during this process.

21. Put the optical filters in for coupler #2. Back reflect them if they're at normal incidence, otherwise be careful to get the angle correct, and then fit the slight steering that will occur.

22. At this point things start to get application specific: if you are going to have waveplates or polarisers in your source, now is the time to put them in, one a time, carefully back--reflecting them, as they'll be useful for the next few steps. However, if you're not going to have them in the system in its final configuration you'll have to find a work-around to control various polarisations.

23. Perform razor-blade scans[9] of all three couplers to optimise the position of the focus. If the experimenter is very lucky, or the foci are very strong you can skip this step, otherwise it will probably be required eventually[10]:

    (a) Mount a razor blade on a translation stage such that it can cut the laser beam inside the interferometer. If this stage is automated, so much the better. Locate the razor blade between the crystal and one of the loop mirrors

    (b) Set the loop HWP for the interferometer to transmit light.

    (c) Set the pump to either H or V.

    (d) Place a power meter at the output port of the interferometer. Again, automated data logging makes this easier.

    (e) Translate the razor blade through the beam, measuring the power at $10 - 15$ points.

    (f) Change the pump to the other polarisation, and repeat the scan.

    (g) Fit $P = A\,\mathrm{erf}\,(w_z(x - x_0)) + C$ to the power vs position data for each direction, where A, C, w_z and x_0 are fitting parameters, P and x are the power and position data, and $\mathrm{erf}(x) = \int_{-\infty}^{x} \exp(-x^2)\,\mathrm{d}x$ is the error function. Depending on your fitting

[9] If you have high-tech solutions to this problem feel free to use them. Our lab has an automatic beam profiler which proved useful for rough alignment, however it cannot fit inside the interferometric loop and so wasn't useful for this step.

[10] Even as I write this I am not sure this is the optimal place in the order of things to perform these scans. It may be correct to optimise each beam's focus as its coupler is placed, or for the pump after the crystal in put into the loop; for many applications you might be able to just skip this step and optimise the focus by eye and by optimising on the count rates: if your pump focus is tight than you can get it into the crystal without much hassle. In my apparatus the focus of the pump beam was very weak ($2w_0 \approx 180\,\mu$m), so optimising its location by eye proved to be too difficult.

package, you may need the ‘erfc’ function(which is $1 - \mathrm{erf}$) depending on the shape of your data. Also, be aware that not all fitting packages define the error function in the same way; this will affect your initial ‘guess’ values for the nonlinear fit and may result in the fit not converging.

(h) Adjust the focus of the pump such that the values of the beam waist, w_z from your fit converge on the same value. Iterate steps 23a to 23g until the waists are the same to within error. Due to the symmetry of the interferometer, the waist should now be in the centre of the loop.

(i) If the centre of the beam, x_0 differs between the two pumping directions your interferometric alignment is off. There are several ways to correct this. You can try adjusting the two mirrors in the loop, though this is tricky. You can also try twisting the SPDC crystal slightly to correct the problem, or, if your loop mirrors are mounted on a translation stage you can use that translation to ensure that the two pumping directions overlap[11].

(j) Repeat this process for the two output couplers and an alignment beam as close as possible to the downconversion wavelength. You can also do some arithmetic at this point to ensure that you’ve made the three foci the expected size: just remember that the waist found here is *not* the waist at the focus. Also check that all three beams are in the same place: that x_0 calculated is the same for each of them in each direction.

24. Set your pump wavelength to H or V, and if present your output analysers to the expected output state (HV or VH).

25. Again, hopefully counts are present in your detectors; now there should be both singles in both channels and coincidences between them. If your timing window is narrow for coincident events don’t forget to scan over a range of time differences or widen the window to find the coincidences if none appear at first but single photons do.

26. Optimise the two couplers to the global maximum of counts for this configurations. The process I use (which may need adaptation depending on the geometry of your couplers) is:

    (a) Choose an output coupler and axis from amongst the available options.

[11] I was told that another group building a similar source had one of their mirrors mounted on a translation stage about a year before I figured out why: I had been told it was for a different purpose entirely. When I was trying to solve a persistent 30 μm offset in my two pump beams I eventually was enlightened that this was the problem they were solving; unfortunately inserting a translation stage at that point was unfeasible.

(b) Iteratively walk the two coupled degrees of freedom on that axis against each other to find the local maximum (for instance, the translation of lens and fibre tip[12] against each other). Ideally, the peak of the coincidences and the singles will be in the same place. If they are not, set the coupler up at the peak of the singles.

(c) Optimise the other axis for the same coupler in the same manner.

(d) Have a quick check on the first axis to make sure things haven't moved too much. If they have your in-principle-orthogonal degrees of freedom aren't; fix your coupler and try again.

(e) Now switch to the other fibre coupler and repeat the process; this time optimise on the coincidence counts.

(f) Walk the macro-motion of each coupler against the other: if you have an overall horizontal motion knob, turn that for both couplers and walk until you find the global optimum, and then the same again the for the vertical motion.

(g) Record the position of every adjustment available to you in a notebook, along with the single and coincidence detection rates.

27. Switch to the opposite pump polarisation. If you have done things at all correctly, there should still be a significant number of counts—the closer they are to those from the other direction, the happier you are. Repeat step 26 to find the global optimum for this pumping configuration.

28. Set the pump to ±45° (and any analysers you have present) and the couplers to the arithmetic mean of the optima found for the two pumping directions.[13]

29. At this point you should have some number of coincident pairs of entangled photons; if you have polarisation analysers present and have a very low coincidence rate flip the pump polarisation by 90°. If the rate of production and heralding efficiency are high enough for your application, you can proceed to 30. Otherwise, iterative improvement is required, as the problem at this point is that the two pumping directions are imperfectly overlapped. I have tried several methods of attack for solving this problem to various degrees of success:

[12] It is a topic for much debate in our lab as to the correct way to build a fibre coupler. Currently, each of our stages has a three-axis translator for the fibre tip and a two-axis translator for the lens, with no angular control. Our previous generation of stages had a common mode translator and a fibre-lens relative motion—these degrees of freedom are, I think, less correlated and so align more quickly, but the mechanisms that allow them are much less repeatable, limiting ultimate performance. If space allows, a fixed lens, three-axis stage for the fibre tip, and two mirrors provides all useful degrees of freedom and is preferred by some experimenters. I cannot recommend more highly that some money be spent on the output fibre couplers: if you have inconsistent travel you will go slowly mad.

[13] I have tried more complicated things than the arithmetic mean to no positive effect, including count-weighted means, attempts to converge on the higher-and lower-count arms, and moving some but not all knobs to an intermediate position—this last due to non-indexed adjusters on some degrees of freedom.

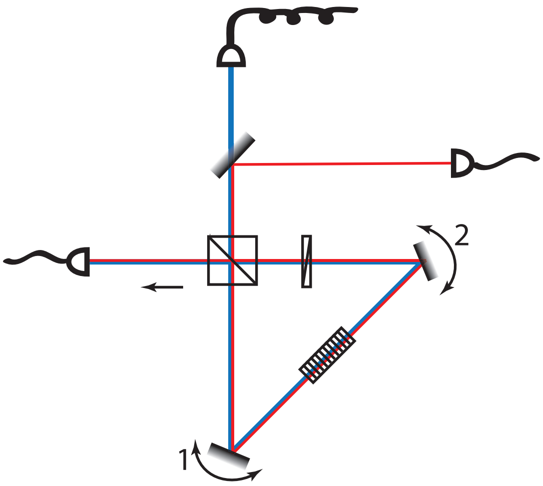

Figure A.2: If the clockwise and counterclockwise outputs are misaligned (but parallel), solving this problem is not trivial. Mirrors 1 and 2 can be walked against each other to do so. Turn mirror one until the clockwise beam is maximally coupled, then turn mirror two until the counterclockwise beam is. Repeat until these maxima are identical, then adjust the fibre coupler until the global maximum is reached. It will tend to be true that the previously found optimum of 1 and 2 will be suboptimal, so repeat.

- If the difference in position of the two beams is small, 10-20 μm, you can tilt a thick optic in the loop to move the two beams nearer each other; the SPDC crystal is a good choice and is actually fairly likely to be slightly out of alignment. Only try this if you have quite good control over the attitude of the SPDC crystal, however.
- Adjust the two interferometric loop mirrors to improve the overlap between the two directions. Take care not to do the opposite of optimising, which I have done on multiple occasions. Due to the lever arm difference between the two mirrors (see figure A.2), adjusting them iteratively to maximise the output counts can either converge on the most overlapped outcome . . . or do the opposite.
- Lastly, if you have one of the mirrors in the loop mounted on a translation stage you can modestly adjust it to overlap the beams in the horizontal direction, which tends to be the one that's more poorly aligned. Translating the mirror in one direction will cause the beams to converge on their mean.

After trying one of these techniques, go back to 26 and try again, hopefully moving toward a global optimum. If you're feeling desperate, or if the foci are obviously wrong, you can also try to optimise the zoom of the two output couplers as you walk the various degrees of freedom on each coupler.

30. Now that we have photon pairs, the last major task is to make them high quality entangled photon pairs: this discussion assumes we want to make maximally entangled singlet states,

but all other states are possible with a bit of work. If you haven't inserted polarising elements in the outputs of the Sagnac either hook the source up to a polarisation analyser or drop some Polaroid sheets on rotation stages into the system to measure the polarisation of the single photons.

31. Set the pump polarisation to generate equal parts $|HV\rangle$ and $|VH\rangle$ photons *at the detectors*. This will often not quite be equal parts pump power in the two pumping directions.

32. Now for the tricky part: setting the pump *phase*. This is set by various things, most controllably the phase between the H and V portions of the pump, but also any phase differences between the two paths around the interferometer. If your system is not very high efficiency, a waveplate in the pump beam, set with it's optic axis vertical or horizontal and then rotated about a vertical axis (*i.e.* such that the angle of incidence upon it changes) is a very controllable way to change the phase of such a system; however it also shifts the H and V beams absolutely and relative to one another. On the other hand, if you have full polarisation control on at least one output the phase of the state can be corrected simply there: just set the other analyser to $|+\rangle = |H\rangle + |V\rangle$, and then correct the one with full polarisation control until maximum extinction is reached. Finally, if neither of these options are available to you, full polarisation control of the pump will also do the trick, again, generate pump polarisations with the same mix of H and V as was found in the previous step, but adjust the phase between them until the output polarisation analysers—set to $|+\rangle$ and $|-\rangle = |H\rangle - |V\rangle$—have a minimum of coincidences. If your 'full polarisation control' of the pump is in the form of a set of bat ears[14], good luck.[15]

At this point, you should have working Sagnac pair source, generating photons of sufficient quality and number as is necessary for your application. Be aware that if you're aiming for extremal performance in any particular characteristic you may be at it for a while—getting the last fractions of performance is both difficult and frustrating[16].

[14] A "Fibre Polarisation Controller", if you're looking to buy one. I've never heard a single person not call them "bat ears", though legend states that some people use a Disney trademark instead.

[15] I suppose some advice to go with that: I have a set of bat ears controlling the pump phase, and a half wave plate on the output to control the polarisation more easily. Ensure that your bat ears are wound correctly (one loop around the first one, two around the second, and three around the third), and that the fibre fits in the bat ears—most are made for unjacketed fibre; if so, and your fibre is jacketed (the yellow layer on typical single mode fibres), strip that off, cut the kevlar threads, and then wind it into the bat ears, where it should sit comfortably. If you do this your bat ears will more closely approximate a quarter-half-quarter waveplate combination and be significantly more predictable in their action.

I have had good results setting the polarisation to a linear one with the bat ears, using the Sagnac loop's HWP as a reference, and then setting the pump to ±45° or close to it to balance the two sets of counts. If everything is set up correctly there should be no phase difference between the two pumping directions, so one of diagonal or antidiagonal pumping should generate singlet states; in practice this is close to true. If it's not close enough, try adjusting only the *last* loop of the bat ears to try and fix it.

[16] If you, as a reader of this thesis, need advice on your source, feel free to contact me; I'd be happy to help.

A.3 Two-photon measurements

If you have photon number resolving detectors or a good in-fibre (preferably polarising) beam-splitter, a significant advantage in finding the collinear outputs can be gained.

Set the pump to pump the loop with light that passes through your loop such that it goes through the crystal and then the half-wave plate, and turn the waveplate 22.5°relative to its normal position, rotating the photons of interest from horizontally and vertically polarised to crossed diagonal polarisations the repeated words made me lose track of the meaning in the sentence[17]. Each of the two photons is thus transmitted or reflected by the PBS with probability 1/2.

If we look at the number of two-photon events received at each coupler, then, they are strongly peaked when the photons being detected are collinearly output by the down-conversion crystal, due to conservation of momentum. Use of the usual tricks to optimise the coupling of biphotons into each coupler can find the global optimum much more quickly than trying to optimise each coupler individually on single photons or both collectively on coincidences.

[17] My grade school teachers would point out that these lines are not the diagonals of anything, and would have docked someone marks for the word ‘anti-diagonal’ which seems popular in this context.

Appendix B

Operation of transition edge sensors

TES are, unfortunately, not plug-and-play devices. Even after you have set up the electronics a fair amount of work remains. In this section, I'll walk through the initial set-up on cool down, and then briefly discuss the day-to-day operation of TES.

B.1 Initial set-up

In order to manipulate and control the TES, an oscilloscope, an ohmmeter and a function generator[1] will be required. You can set up the SQUID amplifiers before the TES have reached superconducting temperatures, as they superconduct at 8 K.

1. Make sure you have a circuit on each detector. Check the resistance of each of the bias, feedback, and SQUID circuits for each detector, and note if you find any open circuits. Other than the first time you set up your detectors or make major modifications this step can be skipped. Each line should have a resistance of a few kilohms: if it is very high or very low (but not open) you have a more complicated problem.

2. Set up the SQUIDs:

   (a) Connect the fridge output of the SQUIDs to the amplifier/bias device, the amplifier's output to the oscilloscope channel two, the function generator to the same channel's feedback connector, and also to the oscilloscope channel one.

   (b) Set the oscilloscope to X vs. Y mode, graphing the two inputs against one another.

   (c) Set the function generator to output a waveform with frequency a few hundred hertz and amplitude a few volts. Adjust the amplitude until a few oscillations of the

[1] Or anything that will generate a wiggly electrical signal at a frequency other than a harmonic of the line frequency.

interference fringe are present.[2]

(d) Adjust the SQUID bias[3] until the interference fringes are as big as possible, see figure B.1. Then reduce the bias a little bit to maximise the steepness of some part of the fringe: this is where the detector will be held during operation. The interference fringes should have amplitude 400-500 mV. If the fringes do not look nice, and the amplitude is lacking, the SQUIDs in the array froze out of phase with each other when they passed through the superconducting transition temperature.

The best way to get them back in phase is to heat the stage they are on above the transition temperature and re-cool them (with no current or magnetic field passing through them). However, a quick-fix can be done by passing a large amount of current through the array, driving it normal via ohmic heating, and then letting it cool[4] again. The coherence will not be as good as on a clean cool-down, but will sometimes be 'good enough', as shown in figure B.1. If the first try doesn't work, try again: the process is quite random.

(e) Disconnect the function generator from the feedback circuit and connect the DC power supply for that circuit. Adjust the DC output until the SQUID sits at the previously identified steepest part of the interference fringe.

(f) Switch the oscilloscope into X vs. T mode and look at the signal. There should be less than 5 mV of noise. If there is excess noise it must be eliminated before the detectors will be useful. Note that you can tune the detectors up first, and then fix the noise problem, but this is more difficult; note also that when we drive the detectors normal the noise will increase. Common sources of noise include:

external signal amplifier (or silver box) being located in a noisy location or with poor ground, try moving it around until a less noisy spot is found;

ground noise from various electronics, try unplugging all but the essential devices and ensure they don't have a ground loop[5];

noise from the ADR magnet from either the leads (if improperly made), and thus acting as antennae, or the power supply;

atmospheric EM noise from lab equipment, found most simply by trial and error: turning equipment off until it goes away, and then removing that equipment as far as possible from the detectors; and

atmospheric EM noise from the pulse tube cooler, mitigated by moving the

[2] If there is no interference fringe at all make sure that the circuit bias is on for the SQUID, the temperature of the SQUIDs is below the superconducting temperature and that oscilloscope is set correctly

[3] The little set screw on the silver box

[4] On NIST-provided devices, this functionality is labelled 'ZAP'.

[5] This noise will be at the line frequency; for Australia this is 50 Hz, while in north america it is 60 Hz

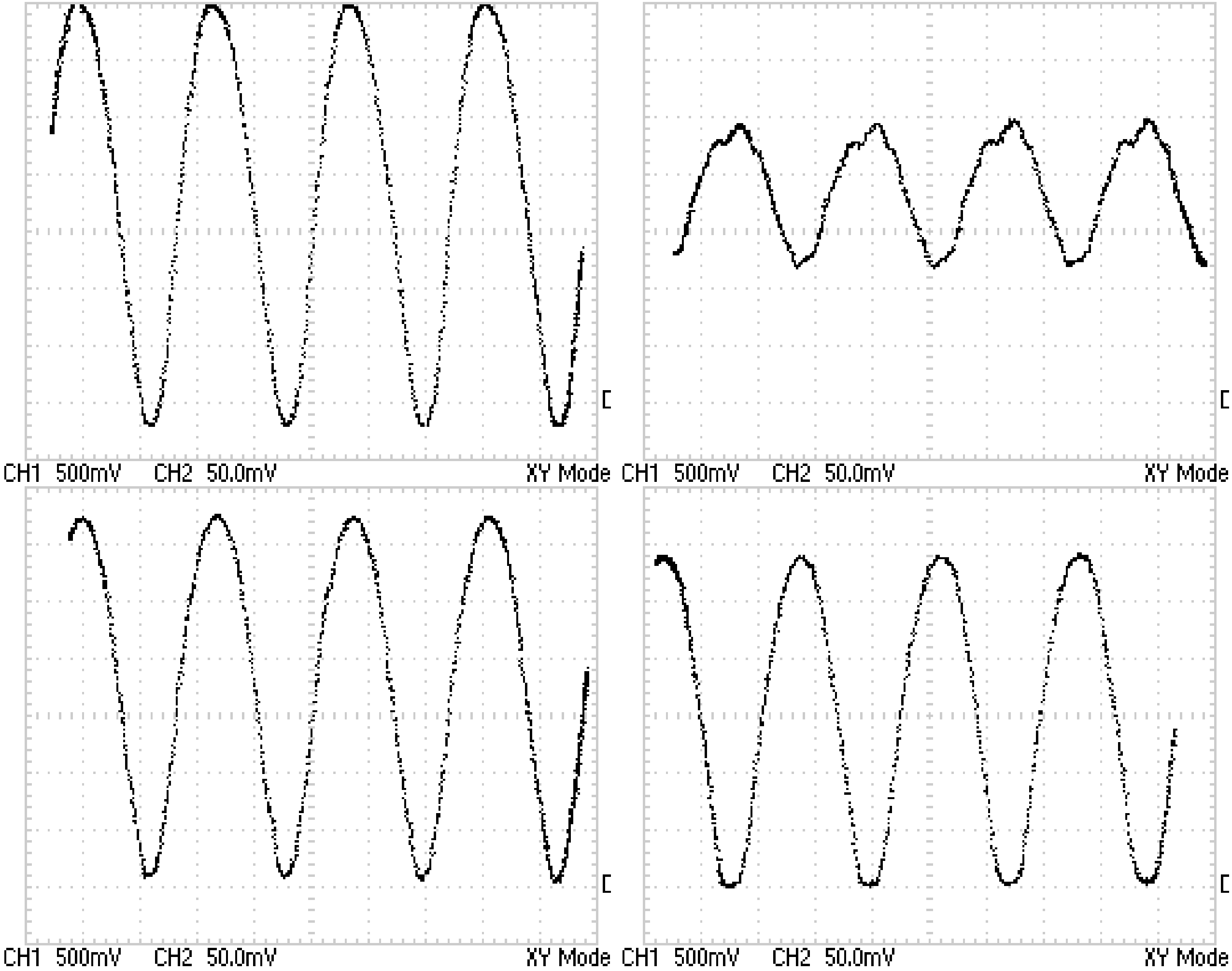

Figure B.1: Four interference fringes from a set of SQUID amplifiers. The horizontal axes are V_{fb}, which is linearly proportional to the magnetic field applied to the SQUIDs. The vertical axis is the voltage response of the SQUID, amplified 10×.

Top left: An example of maximum-amplitude interference fringes for a set of SQUID amplifiers. The minima are at integer multiples of an applied flux quantum.

Top right: A set of SQUID amplifiers that are out of phase. The pure fringes of the various SQUIDs are not adding together perfectly, yielding a slightly 'lumpy' appearance, but also much reduced amplitude and thus slope compared to in--phase operation.

Bottom left: A set of SQUIDs that have been zapped (had a large current put through them) several times to try and regain in-phase behaviour. While almost as large as the top-left trace, they are still slightly irregular rather than a simple sinusoid. This is about as good an outcome as can be obtained by zapping.

Bottom right: A different set of SQUID amplifiers near-optimally tuned. (The slightly lower amplitude is expected variation.) The slight flattening of the bottoms of the fringes tends to increase the local slope slightly above that bottom, which will then be the point where the detectors are held in the ready position.

cooler as far as possible from the detectors, as well as reducing the voltage to the pump therein[6].

3. (Optional) After cooling the TES, connect the function generator to the TES bias input and the oscilloscope, and switch the oscilloscope into X vs. Y mode. A trace similar to that of figure 4.3 should appear. Alternatively, if you set the persistence of the oscilloscope to infinity, and connect the a DC source to the oscilloscope and the TES bias input you can vary the input signal by hand[7]. If there is light reaching the detector the 'detector' region can be noticed as a 'fat' part of this curve. Again, I don't know if this will be possible with the new system. Ensure that the detector region's DC offset doesn't push the signal into the flat part of the SQUID's interference fringe, and if it does adjust the feedback level until it doesn't anymore.

   If no superconducting to normal transition appears, but you do have a reasonable signal then the detector is likely too hot; we recently had an issue where one of our fibres wasn't cooled sufficiently and was heating the TES above the transition temperature. On the other hand, if there is no signal, it is more likely that you have have a broken lead connecting to the detector. The circuit is still closed due to the shunt resistor in parallel to the TES, but without the TES itself being in the circuit.

4. Tune the TES bias:

   (a) Connect the DC source to the bias channel, and set the oscilloscope to Y vs. T mode, displaying the SQUID output with a timebase of about a microsecond.

   (b) Ensure that there's light falling on the detector: usually room lights or a torch pointing at the fibre coupler will do the trick if you don't have actual signal available.

   (c) Add DC until the device goes normal due to surpassing the critical current[8]. Adjust the oscilloscope until you will be able to see the expected TES pulses, which will be about 5 mV by tens of nanoseconds in size, then slowly scan the bias level until you start seeing pulses. At this point you don't need to be able to see the exact features of the pulses, just their existence or otherwise, so a relatively broad view is helpful. Note that on some TES this will be at a lower DC level than the device was at when it made the superconducting to normal transition.

   (d) If there is a lot of electrical noise on the signal, more than about 5 mV, that should get fixed now. 2f, above, lists some common sources of electrical noise.

[6] This voltage should be as low as possible while still pumping once steady state has been reached.

[7] This is how I actually took the traces shown.

[8] While a superconductor has no resistance below the transition temperature, it can only sustain a finite amount of current while superconducting. Once sufficient current is passed through the device, it returns to being a normal resistor.

(e) Set the oscilloscope to be AC coupled, and set the trigger level to trigger on a detection pulse. This can be either a rising or falling pulse depending on where on the SQUID interference fringe you are.

(f) Fine tune the bias level to maximise the signal-to-noise ratio of the pulse. Generally but not invariably this is found at a lower bias than generates a maximally-sized signal.

(g) Tune the feedback level to maximise the signal-to-noise ratio of the pulse. Since the feedback doesn't introduce noise in the same way that the bias does, this tends to mean 'maximise the size of the signal'. After fine-tuning to maximise the pulse, try using the other slope of the SQUID interference fringe as well by adjusting the feedback voltage—as there are many SQUIDs in the SQUID amp, if they are not all perfectly in phase the slopes of the rising and falling sides of the interference fringe may not be identical.

(h) Ultimately, the signal should have signal-to-noise of at least four, which in our system implies a pulse of about 10-20 mV.

5. Connect the signal channel to your data collection system, and adjust that to register your clicks. This will vary highly between different digitisation systems, so consult your manual/local expert.

   I would discuss our system currently in use, but I expect it to be obsolete anon. Note that it's helpful but not critical to keep the detection signals passing through an oscilloscope to keep an eye on things in case of failure.

Repeat the process above for each channel in use. In fact, you can parallelise many of the steps across several detectors if you have the equipment handy. Be aware that your counting/digitising electronics may be a source of noise if additional noise appears on the second or third detector tuned up.

B.2 Daily operations

On a day-to-day basis operations are still more complicated than those of, say, silicon single photon avalanche diodes (Si-SPADs), but relatively simpler than on initial set-up.

The DC level for the SQUID bias (on the amplifier) should remain constant as along as the fridge is cold, but the levels on the TES bias and the feedback channel can vary slightly from day-to-day. Once the system has reached operating temperature for the day, fine tune those two DC levels, then make sure that the timing for the detector hasn't changed. The shape and the height of the pulses varies slightly from day-to-day, which can cause the timing of different channels to become out of sync.

Appendix C

Paper: Conclusive quantum steering

This appendix consists of the paper that initially presented the results of chapter 5.

nature COMMUNICATIONS

OPEN

ARTICLE

Received 3 Aug 2011 | Accepted 30 Nov 2011 | Published 10 Jan 2012

DOI: 10.1038/ncomms1628

Conclusive quantum steering with superconducting transition-edge sensors

Devin H. Smith[1,2], Geoff Gillett[1,2], Marcelo P. de Almeida[1,2], Cyril Branciard[2], Alessandro Fedrizzi[1,2], Till J. Weinhold[1,2], Adriana Lita[3], Brice Calkins[3], Thomas Gerrits[3], Howard M. Wiseman[4], Sae Woo Nam[3] & Andrew G. White[1,2]

Quantum steering allows two parties to verify shared entanglement even if one measurement device is untrusted. A conclusive demonstration of steering through the violation of a steering inequality is of considerable fundamental interest and opens up applications in quantum communication. To date, all experimental tests with single-photon states have relied on post selection, allowing untrusted devices to cheat by hiding unfavourable events in losses. Here we close this 'detection loophole' by combining a highly efficient source of entangled photon pairs with superconducting transition-edge sensors. We achieve an unprecedented ~62% conditional detection efficiency of entangled photons and violate a steering inequality with the minimal number of measurement settings by 48 s.d.s. Our results provide a clear path to practical applications of steering and to a photonic loophole-free Bell test.

[1] Centre for Engineered Quantum Systems and Centre for Quantum Computation and Communication Technology (Australian Research Council), University of Queensland, 4072 Brisbane, Queensland, Australia. [2] School of Mathematics and Physics, University of Queensland, 4072 Brisbane, Queensland, Australia. [3] National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305, USA. [4] Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, 4111 Brisbane, Queensland, Australia. Correspondence and requests for materials should be addressed to D.H.S. (email: smith@physics.uq.edu.au).

Quantum entanglement enables unconditionally secure communication and powerful devices such as quantum computers. In their strongest form, the correlations associated with entanglement rule out locally causal world views via tests of Bell inequalities[1]. In a weaker regime, quantum correlations can still be harnessed to steer quantum states, demonstrating that two parties, Alice and Bob, share entanglement even if one party is untrusted[2]. Quantum steering was originally introduced by Erwin Schrödinger[3], in reaction to the Einstein, Podolsky and Rosen (EPR) 'paradox'[4]; it describes the ability to remotely prepare different ensembles of quantum states by performing measurements on one particle of an entangled pair, demonstrating the paradox. Depending on the measurement and its random outcome, the remote system is prepared in a different state; however, the unconditioned remote state remains unaffected, thus preventing any possible superluminal signalling. Interestingly, steering and Heisenberg's uncertainty principle have recently been linked to Bell non-locality[5].

The original form of the EPR paradox was demonstrated experimentally with atomic ensembles[6], continuous-variable states of light[7,8] and position-momentum entangled single photons[9]. More recently, quantum steering was redefined in a quantum information context in ref. 2, promising new applications such as quantum communication using untrusted devices[10]. This new formalization also allows a strict comparison between the concepts of Bell non-locality, steering and entanglement[2]: Bell non-locality requires steering, which in turn requires entanglement. In analogy to entanglement witnesses[11] and Bell inequalities[12], one can derive experimental criteria[13] to demonstrate steering: steering inequalities impose limits on the observable correlations that can be explained without the need to invoke quantum steering. An experimental violation of a steering inequality was recently reported in ref. 14.

Steering—in a more general sense—has also been shown to be one of two contributors to the degree of Bell non-locality, the other being the uncertainty principle[5]. In this sense, there can be perfect steering in both quantum mechanics and in local hidden-variable theories—their uncertainty relations dictate their different degrees of non-locality. We demonstrate here states with high steerability, in contrast to states in deterministic classical mechanics that have no uncertainty and no steerability.

We define the steering task in Figure 1: Alice and Bob receive quantum states from a source and measure them using randomly chosen measurements from a prearranged set; if the observed correlations violate a steering inequality, then Alice and Bob will be convinced that their shared states were entangled. This holds true even if Alice and Bob trust neither the source nor Alice's measurement device.

Similarly to the case of Bell inequalities, a conclusive violation of a steering inequality requires that the experiment does not suffer from any relevant loopholes. When one party has untrusted equipment, the so-called detection loophole[15] in particular is critical: if Alice and Bob have to post select their data on Alice's detected events, then low efficiencies enable her measurement devices to cheat by dropping unfavourable results—in the context of quantum key distribution, for instance, this would allow the untrusted supplier of the devices to access the key. The fair sampling assumption invoked in ref. 14, for instance, is not satisfactory for such untrusted devices.

Here we close the detection loophole by using an entangled photon source with high pair collection efficiency[16,17] and highly efficient transition-edge sensors (TESs)[18]. We test a steering inequality that naturally accounts for Alice's non-detected events, and violate it by at least 48 standard deviations with the minimum number of two measurement settings and by more than 200 standard deviations for measurements in three different bases.

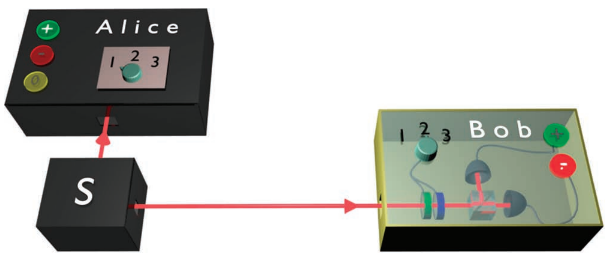

Figure 1 | Conceptual depiction of quantum steering. Alice and Bob receive particles from a black box (the source, *S*) and want to establish whether these are entangled. From a prearranged set, they each choose measurements to be performed on their respective particles. Bob's measurement implementation is trusted, but this need not be the case for Alice's; her measurement device is also treated as a black box from which she gets either a 'conclusive', $A_i = \pm 1$, or a 'non-conclusive' outcome, $A_i = 0$. To demonstrate entanglement, Alice and Bob need to show that she can steer his state by her choice of measurement. They can do so through the violation of a steering inequality: whenever Bob's apparatus detects a particle, Alice needs to provide her measurement result. If the recorded correlations of their measurement results surpass the bound imposed by the steering inequality, Alice and Bob have conclusively proven the entanglement of their particles.

Results

A quadratic steering inequality for qubits. To demonstrate steering, Alice and Bob need to be able to freely choose and perform different measurements; we consider the case where each of them can perform $N=2$ or 3 measurements, labelled $i,j=1,2$ or 3, with *a priori* binary outcomes $A_i,B_j=\pm 1$ as shown in Figure 1. As Bob trusts his measuring device his measurement can be described by a well-characterized quantum observable $\hat{B}_j$. He considers only the cases where his measurement gives him a conclusive result, that is, when at least one of his detectors clicks—if both click, Bob outputs a random result. In contrast, Alice's devices are not trusted and her measurement apparatus is considered a black box, which is polled whenever Bob receives a result. It returns outcomes $A_i = \pm 1$, indicating conclusive measurement results, or $A_i = 0$ when no or both detectors fire. Alice must output a result whenever Bob registers an event, thus any of her inconclusive results cannot be discarded from further analysis.

The correlation observed by Alice and Bob can be described by the probability distribution $P(A_i=a,\ B_j=b)$, with $a=\pm 1$ or 0, and $b=\pm 1$. If Bob receives a state that is not entangled to Alice's the set of possible correlations will be restricted, as shown below. First, we define Bob's expectation value for a measurement conditioned on Alice's result, measuring the amount that her results steer his outcomes:

$$\langle \hat{B}_i \rangle_{A_i=a} \equiv P(B_i=+1 \,|\, A_i=a) - P(B_i=-1 \,|\, A_i=a). \tag{1}$$

Averaging $\langle \hat{B}_i \rangle_{A_i=a}$ over Alice's results, we define Bob's average expectation

$$E[\langle \hat{B}_i \rangle^2_{A_i}] \equiv \sum_{a=\pm 1,0} P(A_i=a)\langle \hat{B}_i \rangle^2_{A_i=a}. \tag{2}$$

As shown in the Methods section, if the correlation P could be explained by the source sending Bob an unentangled two-level system (qubit)—that is, in the terminology of ref. 2, if the correlation admits a 'local hidden state' model—and if Bob implements qubit measurements in $N=2$ or 3 mutually unbiased bases, for instance of the Pauli $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ operators, then the following steering inequality holds:

$$S_N \equiv \sum_{i=1}^{N} E[\langle \hat{B}_i \rangle^2_{A_i}] \le 1, \tag{3}$$

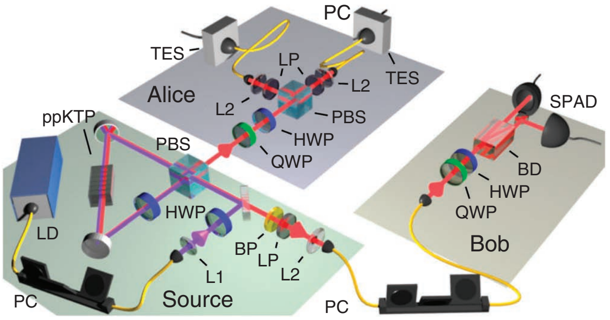

Figure 2 | Experimental scheme. Polarization-entangled two-photon states are generated in a periodically poled 10 mm KTiOPO$_4$ (ppKTP) crystal inside a polarization Sagnac loop[16,17]. The continuous wave, grating-stabilized 410-nm pump laser (LD) is focussed into this crystal with an aspheric lens (L1, f = 4.0 mm) and its polarization is set with a fibre polarization controller (PC) and a half-wave plate (HWP), controlling the entangled output state[16]. Bob filters his output photon with a long-pass glass filter (LP) and a 3-nm band-pass filter (BP), before collecting it with an aspheric lens (L2, f = 18.4 mm) into a single-mode fibre. He performs his measurement in an external fibre bridge, with a combination of a quarter-wave plate (QWP), HWP, a polarizing beam displacer (BD) and multi-mode-fibre-coupled single-photon avalanche diodes (SPADs). To minimize loss, Alice performs her measurement directly at the source using a QWP, HWP and a polarizing beamsplitter (PBS), followed by a LP filter and fibre collection with focussing optics identical to Bob's, finally detecting her photons with highly efficient superconducting transition-edge sensors (TESs)[18].

where S_N is the steering parameter for N bases. Note that the upper bound above depends crucially on Bob's measurement settings, which in experimental implementation will not be perfectly orthogonal, nor perfectly projective; we detail in the Methods section how the bound must be corrected to account for experimental imperfections.

Quantum mechanics allows a violation of inequality (3), which thus implies steering. To get a first insight, suppose that Alice and Bob share Werner states of visibility V, $\rho = V|\psi^-\rangle\langle\psi^-| + (1-V)\mathbb{1}/4$, where $|\psi^-\rangle$ is the Bell singlet state, and that Alice implements the same measurements as Bob. Then, due to the anti-correlation of the singlet state when measured in the same basis, $\langle\hat{B}_i\rangle_{A_i=\pm1} = \mp V$: this illustrates that Alice can steer Bob's state to be aligned with her measurement axis, limited by the visibility of the shared state. If Alice has a probability η of getting a conclusive outcome whenever Bob gets one, then $E[\langle\hat{B}_i\rangle^2_{A_i}] = \eta V^2$. This means that the steering inequality (3) will be violated if

$$\eta V^2 > 1/N. \tag{4}$$

Satisfying the requirements given by equation (4) in a photonic architecture is challenging. For the minimal set of N=2 measurement settings, an experimental test of the steering inequality (3) requires, even for a pure entangled singlet state with visibility V=1, that Alice detects a signal more than η>50% of the times Bob requests a response. To reach these requirements, the experimental apparatus has to be carefully optimized.

Experimental setup. We performed our experiment using entangled photons created in a polarization Sagnac source based on spontaneous parametric downconversion[16,17], see Figure 2. This source design meets two crucial requirements; a high entangled-pair collection efficiency and near-ideal polarization entanglement.

We followed ref. 17 in the basic design of our source. To maximize the conditional coupling between Alice and Bob's collection apparatus, we optimized the pump and collection spots based on ref. 19, with the optimum found at using pump spot and collection mode diameters of 200 and 84 µm in the crystal, respectively. With these parameters, we achieved a typical pair detection efficiency of 40% measured with standard single-photon avalanche diodes (SPADs), whose detection efficiency was estimated to be 50% at 820 nm, implying a collection efficiency of 80%. Owing to the asymmetry of the steering task, the source and detection system do not have to be symmetric. For example, in our setup Alice does not employ narrow-band filters; this choice increases her overall background, but reduces her loss, thus increasing the detection efficiency conditioned on Bob's measurement.

Another key requirement is high photon detection efficiency. The conditional detection probability η is upper bounded by the performance of Alice's photon detectors, and therefore would not even in a loss-less, noise-free case allow us to meet the requirements of equation (4) with our SPADs and two measurement settings; in our experiment, Alice thus employs highly efficient TESs[18]. These detectors utilize a layer of superconducting tungsten kept in the transition temperature range and offer a combination of photon number resolution and high detection efficiency of up to 95% at 1,550 nm, while being virtually free of dark counts[18]. Our detectors were optimized for 810 nm with an optical cavity similar to that presented in an earlier work[18], with an estimated detection efficiency for 820 nm photon in the 1,550 nm single-mode SMF-28 fibre connected to this cavity to be larger than 97%. In practice, the measured detection efficiencies of our two TES were 1.50 and 1.56 times higher than the efficiency of our reference SPAD at 820 nm. The dominant source of optical loss, which leads to these less-than-optimal figures, was a splice between the single-mode 820-nm fibres connected to the source and the fibres connected to the TES, which were single mode at 1,550 nm.

The TESs were operated between 40 and 75 mK and yielded analogue output pulses with a rise time of ~320 ns and jitter of ~78 ns. To detect coincidences between the TES signals and the TTL pulses generated by the SPADs, each amplified TES signal was digitized with a constant fraction discriminator. Because the TESs rethermalize with a relaxation period of ~2 ms after each detection event, the non-number resolving discriminators were set to impose a dead time of the same length to avoid false detections. To match the delay caused by the TES detection system, Bob's SPAD signals were delayed by ~450 ns. Coincident events were then detected with a field-programmable gate array with a timing window of 98 ns.

The long dead time period imposed by our electronics leads to a rate-dependent loss and we therefore operated the source at comparatively low rates of photon-pair creation. We achieved optimal conditional detection efficiency at a laser pump power of 250 µW, generating ~12 kHz of single photons in each TES channel. At this rate, the loss due to dead time was ~2.5%.

Experimental violation of our steering inequality. We produced the polarization-entangled singlet state $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$, where $|H\rangle$ and $|V\rangle$ represent single horizontal and vertical polarized photons, respectively, and performed separate measurements in 2 and 3 different bases (N=2, 3, with measurements of $\hat{X}$, $\hat{Y}$ and $\hat{Z}$). The discrete probability distribution for Alice and Bob's correlations, $P(A_i = a, B_j = b)$, is shown in Figure 3a. From these, we first estimated an averaged heralding efficiency η and entangled state visibility V and compared them to the theoretical minimum requirements, equation (4), in Figure 3b. The plot indicates a conclusive, detection-loophole-free demonstration of steering.

Indeed, for the steering parameter S_3 defined in (3), we obtained

$$S_3 = 1.7408 \pm 0.0017,$$

where the uncertainty (1 standard deviation) was calculated by standard propagation of the Poissonian photon-counting statistics.

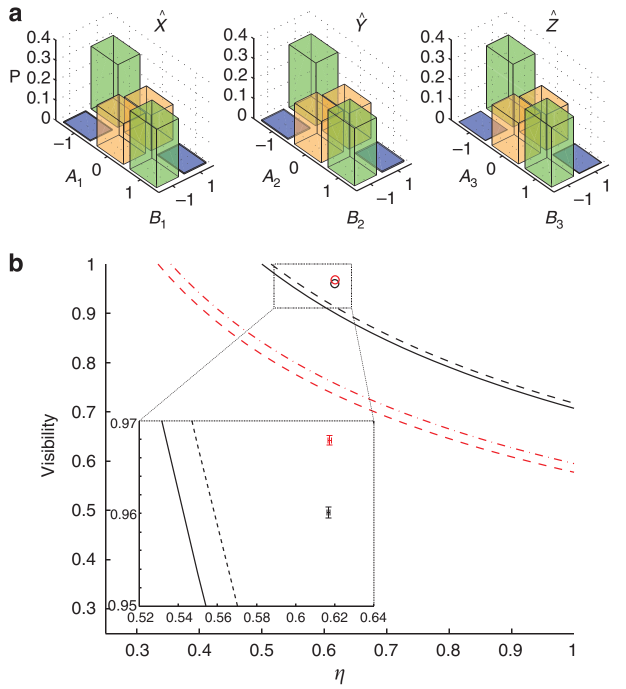

Figure 3 | Experimental violation of a steering inequality. (**a**) Probability distributions $P(A_i=a,B_i=b)$ for the S_3 measurements $\hat{X}$, $\hat{Y}$ and $\hat{Z}$, calculated by normalizing the registered coincident events for each measurement setting to the total count numbers. The green and blue bars represent correlations that indicate the quality of the shared entangled state. The orange bars represent events that Alice failed to detect. Error bars are too small to be seen on this scale. For S_2, we used the data obtained from the measurements of $\hat{X}$ and $\hat{Y}$. (**b**) Theoretical visibility required to violate steering inequalities for $N=3$ (red dashed line) and $N=2$ (black line) for a given efficiency η. Our measurement clearly violates this bound, with an averaged visibility of $V=0.9678\pm0.0005$ at a mean heralding efficiency of $\eta=0.6175\pm0.0008$ for the $N=3$ measurements (red) and $V=0.9601\pm0.0006$, $\eta=0.6169\pm0.0008$ for $N=2$ (black). All error bars (1 s.d.) were calculated assuming Poissonian photon-counting statistics. The correction to the analytic bound of inequality (3) due to measurement imprecision (calculated in the Methods section) is shown by the dash-dotted red line for S_3 and the dashed black line for S_2.

The corrected bound, due to imprecision in Bob's measurements and as calculated in the Methods section, was 1.062±0.003. This corresponds to a violation of inequality (3) by more than 200 standard deviations.

For $N=2$, the corresponding corrected bound of inequality (3) was 1.029±0.0019. We obtained the value

$$S_2=1.1410\pm0.0014$$

for the experimental steering parameter, yielding a violation of the steering inequality by 48 standard deviations.

Discussion

Our highly efficient system allows us to firmly close the detection loophole in this demonstration of quantum steering, achieving the highest ever reported heralding efficiency for entangled photons, $\eta\approx62\%$. The experimental violation of inequality (3) has a quite intuitive interpretation: it shows that Alice can, at her will, steer Bob's qubit state to be preferably polarized along any of the three axes of the Bloch sphere, as demonstrated in Figure 3a.

While we have closed the detection loophole, we have not addressed the locality and freedom of choice loopholes[20] in this work; closing these would require Alice and Bob's choice and implementation of measurements to be space-like separated, as demonstrated in a very recent experiment reported in ref. 21. For practical purposes in quantum communication, however, these loopholes are typically not problematic[22]: it is a necessary assumption that Alice and Bob can choose their measurements independently of the state preparation, and that no unwanted information leaks from Alice and Bob's laboratories.

Besides the criteria employed here there are others that can be used to demonstrate steering[13,23]. If Alice cannot achieve the high heralding efficiencies obtained in our experiment, some of these may be advantageous: as recently shown in ref. 24, generalizing the linear criteria of ref. 14 allows for steering with arbitrarily high losses. However, these require a larger number of different measurement settings up to $N=16$ in the experiment reported in ref. 23. Our choice to test inequality (3) was motivated by its simplicity in how it naturally accounts for Alice's detection inefficiencies, and by its minimality in the number of settings. Note that $N=2$ is the number of settings initially discussed by EPR; it is also the canonical number of settings in applications to quantum cryptography[10].

Increasing Alice's detection efficiency above 65.9% will enable steering to be used for quantum key distribution where one party distrusts their apparatus[10,25]; our experiment thus constitutes an important step towards practical applications of quantum steering. Furthermore, our results imply that a fully loophole-free photonic Bell test seems to be within arm's reach. While the symmetric photon pair detection efficiency for our setup is somewhat lower than the conditional detection probability η, it is not far below the $66.\bar{6}\%$ limit required to violate a Clauser-Horne inequality[26] with non-maximally entangled states[27]. Although still a technological challenge, it is now conceivable to surpass this efficiency in the near future, while simultaneously addressing the locality and freedom-of-choice loopholes such as demonstrated in ref. 20. Note that detection-loophole-free Bell experiments have already been performed in ionic[28] and solid-state[29] systems. These systems however present significant difficulties in reaching the required spatial separation to simultaneously close the locality loophole.

Methods

Proof of inequality (3). Inequality (3) is equivalent to previously derived variance criteria[13,30]. For completeness, we give here a simple and self-contained proof.

If the observed correlation can be explained by the source sending non-entangled states to Alice and Bob, then the probability distribution P can be decomposed in the form

$$P(A_i=a,B_j=b)=\sum_\lambda q_\lambda\, P_\lambda(A_i=a)\,P^Q_{\rho\lambda}(B_j=b),$$

where λ describes the source preparation, used with probability q_λ (such that $q_\lambda\geq0$, $\sum_\lambda q_\lambda=1$—note that the sum could in principle be continuous and infinite): it specifies Alice's response function $P_\lambda(A_i{=}a)$ implemented by her (untrusted) measurement device, and the state ρ_λ sent to Bob. The trusted observable $\hat{B}_j$, chosen and fixed by Bob, then generates Bob's response function $P^Q_{\rho\lambda}(B_j=b)$ as quantum mechanics predicts.

From the above decomposition, and defining

$$q_{\lambda|A_i=a}\equiv q_\lambda\frac{P_\lambda(A_i=a)}{P(A_i=a)},$$

such that, as before, $q_{\lambda|A_i=a}\geq0$ and $\sum_\lambda q_{\lambda|A_i=a}=1$, we get $P(B_i=b\,|\,A_i=a)=\sum_\lambda q_{\lambda|A_i=a}P^Q_{\rho\lambda}(B_i=b)$ and

$$\langle\hat{B}_i\rangle_{A_i=a}=\sum_\lambda q_{\lambda|A_i=a}\langle\hat{B}_i\rangle_{\rho\lambda}.$$

By the co-nvexity of the square,

$$\langle\hat{B}_i\rangle^2_{A_i=a}\leq\sum_\lambda q_{\lambda|A_i=a}\langle\hat{B}_i\rangle^2_{\rho\lambda},$$

which leads to

$$E[\langle \hat{B}_i \rangle_{A_i}^2] \leq \sum_\lambda q_\lambda \langle \hat{B}_i \rangle_{\rho\lambda}^2 .$$

Now, for any 1-qubit state ρ_λ, and for 3 mutually unbiased observables $\hat{B}_i$, one has (due to an uncertainty relation[31])

$$\sum_{i=1}^{3} \langle \hat{B}_i \rangle_{\rho\lambda}^2 \leq 1.$$

Together with the previous inequality and the normalization $\sum_\lambda q_\lambda = 1$, we obtain inequality (3),

$$S_N \equiv \sum_{i=1}^{N} E[\langle \hat{B}_i \rangle_{A_i}^2] \leq 1$$

for $N=3$; the case for $N=2$ follows trivially. The maximal violation of a steering inequality arises from the unbiased observables maximizing local uncertainty[31], reducing the classical bound, while the measurement results at the two locations represent perfect steering of states, maximizing the quantum bound.

Correcting for Bob's imperfect measurements. In the steering protocol no assumption is made about Alice's measurement device, which therefore need not be carefully characterized. Inequality (3) is, however, highly dependent on Bob's measurements: it is only valid when Bob measures mutually unbiased observables on qubits. In a practical experiment, however, Bob will not measure along perfectly mutually unbiased bases, and his operators may not act on a two-dimensional system only. We show now that the parameter S_N can still be used to demonstrate steering, but the upper bound in (3) must be adapted according to Bob's actual measurement.

Let us start by giving a more accurate description of the measurement Bob performs in our experiment. First, he uses quarter- and half-wave plates, which define a direction (that is, a unit vector) $\vec{b}$ on the Bloch sphere, representing his choice of basis. The beam displacer (BD) then separates the H and V polarizations: a fraction $t \simeq 1$ of the H polarization goes to its first output channel, and later on to the "$+1$" detector, while a fraction $1-t \ll 1$ (in our experiment, $1-t \leq 10^{-5}$) goes to the second output channel, and to the "-1" detector. We can assume that, symmetrically, a fraction t of the V polarization goes to the second output channel, while a fraction $1-t$ goes to the first output channel, as we utilize a calcite BD as our polarizing element; its intrinsic birefringence maps polarization into different spatial modes, which is a fundamentally symmetric effect[32]. Note that other polarizing elements require a slightly more thorough analysis. We finally denote by η_+ and η_- the overall detection efficiencies of the $+1$ and -1 detectors (SPADs), respectively, including all losses in Bob's lab, including coupling and detection losses.

For a single-photon state entering Bob's lab, represented by a vector $\vec{u}$ in the Bloch sphere, the probability that it gives a click on the $+1$ or -1 detector is then

$$P_B(\pm|\vec{b}) = \frac{\eta_\pm}{2}[1 \pm (2t-1)\vec{b}\cdot\vec{u}].$$

It follows that

$$\begin{aligned} P_B(+|\vec{b}) + P_B(-|\vec{b}) &= \frac{\eta_+ + \eta_-}{2} + \frac{\eta_+ - \eta_-}{2}(2t-1)\vec{b}\cdot\vec{u} \\ &\geq \frac{\eta_+ + \eta_-}{2} - \left|\frac{\eta_+ - \eta_-}{2}\right| = \min(\eta_+,\eta_-) \end{aligned}$$

and

$$\begin{aligned} |P_B(+|\vec{b}) - P_B(-|\vec{b})| &= \left|\frac{\eta_+ - \eta_-}{2} + \frac{\eta_+ + \eta_-}{2}(2t-1)\vec{b}\cdot\vec{u}\right| \\ &\leq \left|\frac{\eta_+ - \eta_-}{2}\right| + \frac{\eta_+ + \eta_-}{2}|\vec{b}\cdot\vec{u}| \\ &= \max(\eta_+,\eta_-)[\delta + (1-\delta)|\vec{b}\cdot\vec{u}|] \end{aligned}$$

with $\delta \equiv \dfrac{|\eta_+ - \eta_-|}{2\max(\eta_+,\eta_-)}$. Hence, defining $w \equiv \dfrac{\max(\eta_+,\eta_-)}{\min(\eta_+,\eta_-)}$, we get

$$|\langle B \rangle| = \frac{|P_B(+|\vec{b}) - P_B(-|\vec{b})|}{P_B(+|\vec{b}) + P_B(-|\vec{b})} \leq w[\delta + (1-\delta)|\vec{b}\cdot\vec{u}|]$$

and by convexity,

$$\langle B \rangle^2 \leq w^2[\delta + (1-\delta)(\vec{b}\cdot\vec{u})^2].$$

Consider now $N=2$ or 3 measurement directions $\vec{b}_i$, such that $|\vec{b}_i \cdot \vec{b}_j| \leq \varepsilon$ for all $i{\neq}j$, for some $\varepsilon > 0$ quantifying the non-orthogonality of the N directions. One can show that for all $\vec{u}$ in the Bloch sphere,

$$\sum_{i=1}^{N} (\vec{b}_i \cdot \vec{u})^2 \leq 1 + (N-1)\varepsilon.$$

Indeed the worst case is obtained when the N vectors $\vec{b}_i$ are such that $\vec{b}_i \cdot \vec{b}_j = \varepsilon$ for all $i{\neq}j$, and when $\vec{u}$ is a unit vector equidistant to the $\vec{b}_i$, which gives the upper bound above.

Following the proof of inequality (3), we now obtain, for Bob's actual measurements, the steering inequality

$$S_N \leq w^2[1 + (N-1)(\delta + \varepsilon - \delta\varepsilon)]. \qquad (5)$$

In our experiment, the ratio of detection efficiencies in Bob's two detectors was $w = \eta_+/\eta_- = 1.0115 \pm 0.0007$. We estimated the orthogonality ε of Bob's measurements by inserting a large ensemble of different linear polarization states into Bob's measurement device, fully characterizing the two wave-plates and the relative coupling. For the $N=3$ measurement settings, we can take epsilon to be the maximum of all three scalar products $|\vec{b}_i \cdot \vec{b}_j|$; we found $\varepsilon = 0.0134 \pm 0.0007$ in that case. For the test with $N=2$ settings, we used the two most orthogonal settings, $\hat{X}$ and $\hat{Y}$, which gave $\varepsilon = (1.3 \pm 1.5) \times 10^{-4}$. From (5), this yields bounds of 1.0291 ± 0.0019 and 1.062 ± 0.003 for S_2 and S_3, respectively, as quoted in the main text.

Other experimental imperfections include dark counts and background of the detectors at tens of hertz, compared with a rate of ~12 kHz total detected events for Bob. These will however only introduce some white noise into Bob's data, and cannot increase the bound in the steering inequality.

The previous calculations assumed that Bob received qubit states, encoded in the polarization of single photons. This is however not guaranteed, and the source could indeed send multiphoton states. This problem can be treated if it is assumed that Bob has perfectly orthogonal measurements, linear detectors with equal efficiencies and randomly assigns outcomes for measurements with multiple detections. Indeed, using a squashing operation[33]—which maps a larger Hilbert space into a qubit space—it can be shown that treating the outputs of our measurements as representing qubit states will in no cases allow a state without bipartite entanglement to violate steering inequality (3). Although it is not straightforward to extend the results of ref. 33 to imperfectly orthogonal measurements, intuitively it is clear that the assignment of random outcomes to multiple detection events will reduce Alice and Bob's correlations, and will not help Alice's untrustworthy devices to increase the steering parameter S_N. This intuition holds even if the detector efficiencies are not balanced, accounted for in our treatment of imprecise measurements, inequality (5). Given this, in the experiment Bob assigned a random outcome to the 0.07% of events that were double clicks.

It is an open question whether squashing could also to some extent account for more realistic detectors with potential nonlinear response[34]. This effect—and other detector imperfections—could potentially be exploited by an untrusted party[35]. While these attacks are not an issue for a laboratory steering test similar to ours, they should definitely be considered in the design of any real-world quantum communication scheme, including future ones relying on steering inequalities.

References

1. Bell, J. *Speakable and Unspeakable in Quantum Mechanics* 2nd edn (Cambridge University Press, 2004).
2. Wiseman, H. M., Jones, S. J. & Doherty, A. C. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. Lett.* **98,** 140402 (2007).
3. Schrödinger, E. Die gegenwärtige Situation in der Quantenmechanik. *Naturwissenschaften* **23,** 807–812; 823–828; 844–849 (1935).
4. Einstein, A., Podolsky, B. & Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47,** 777–780 (1935).
5. Oppenheim, J. & Wehner, S. The uncertainty principle determines the nonlocality of quantum mechanics. *Science* **330,** 1072–1074 (2010).
6. Hald, J., Sørensen, J., Schori, C. & Polzik, E. Spin squeezed atoms: a macroscopic entangled ensemble created by light. *Phys. Rev. Lett.* **83,** 1319–1322 (1999).
7. Silberhorn, C. *et al.* Generation of continuous variable Einstein-Podolsky-Rosen entanglement via the Kerr nonlinearity in an optical fiber. *Phys. Rev. Lett.* **86,** 4267–4270 (2001).
8. Bowen, W., Schnabel, R., Lam, P. & Ralph, T. Experimental investigation of criteria for continuous variable entanglement. *Phys. Rev. Lett.* **90,** 43601 (2003).
9. Howell, J. C., Bennink, R. S., Bentley, S. J. & Boyd, R. W. Realization of the Einstein-Podolsky-Rosen paradox using momentum- and position-entangled photons from spontaneous parametric down conversion. *Phys. Rev. Lett.* **92,** 210403 (2004).
10. Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V. & Wiseman, H. M. One-sided device-independent quantum key distribution: security, feasibility and the connection with steering. Preprint at http://arXiv.org/abs/1109.1435 (2011).
11. Horodecki, M., Horodecki, P. & Horodecki, R. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* **223,** 1–8 (1996).
12. Bell, J. S. On the Einstein-Podolsky-Rosen paradox. *Physics* **1,** 195–200 (1964).
13. Cavalcanti, E. G., Jones, S. J., Wiseman, H. M. & Reid, M. D. Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox. *Phys. Rev. A* **80,** 032112 (2009).

14. Saunders, D. J., Jones, S. J., Wiseman, H. M. & Pryde, G. J. Experimental EPR-steering using Bell-local states. *Nat. Phys.* **6,** 845–849 (2010).
15. Pearle, P. M. Hidden-variable example based on data rejection. *Phys. Rev. D* **2,** 1418–1425 (1970).
16. Kim, T., Fiorentino, M. & Wong, F. Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer. *Phys. Rev. A* **73,** 12316 (2006).
17. Fedrizzi, A., Herbst, T., Poppe, A., Jennewein, T. & Zeilinger, A. A wavelength-tunable fiber-coupled source of narrowband entangled photons. *Opt. Express* **15,** 15377–15386 (2007).
18. Lita, A. E., Miller, A. J. & Nam, S. W. Counting near-infrared single-photons with 95% efficiency. *Opt. Express* **16,** 3032–3040 (2008).
19. Bennink, R. Optimal collinear Gaussian beams for spontaneous parametric down-conversion. *Phys. Rev. A* **81,** 053805 (2010).
20. Scheidl, T. *et al.* Violation of local realism with freedom of choice. *Proc. Natl Acad. Sci. USA* **107,** 19708–19713 (2010).
21. Wittmann, B. *et al.* Loophole-free quantum steering. Preprint at http://arXiv.org/abs/1111.0760 (2011).
22. Pironio, S. *et al.* Device-independent quantum key distribution secure against collective attacks. *New J. Phys.* **11,** 045021 (2009).
23. Walborn, S. P., Salles, A., Gomes, R. M., Toscano, F. & Souto Ribeiro, P. H. Revealing hidden Einstein-Podolsky-Rosen nonlocality. *Phys. Rev. Lett.* **106,** 130402 (2011).
24. Bennet, A. J. *et al.* Arbitrarily loss-tolerant Einstein-Podolsky-Rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. Preprint at http://arXiv.org/abs/1111.0739 (2011).
25. Ma, X. & Lütkenhaus, N. Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD Preprint at http://arXiv.org/abs/1109.1203 (2011).
26. Clauser, J. F. & Horne, M. A. Experimental consequences of objective local theories. *Phys. Rev. D* **10,** 526–535 (1974).
27. Eberhard, P. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A* **47,** 747–750 (1993).
28. Rowe, M. A. *et al.* Experimental violation of a Bell's inequality with efficient detection. *Nature* **409,** 791–794 (2001).
29. Ansmann, M. *et al.* Violation of Bell's inequality in Josephson phase qubits. *Nature* **461,** 504–506 (2009).
30. Cavalcanti, E. G., Drummond, P. D., Bachor, H. A. & Reid, M. D. Spin entanglement, decoherence and Bohm's EPR paradox. *Opt. Express* **17,** 18693–18702 (2009).
31. Wehner, S. & Winter, A. Higher entropic uncertainty relations for anti-commuting observables. *J. Math. Phys.* **49,** 062105 (2008).
32. Hecht, E. *Optics* 4 edn (Addison Wesley, 2002).
33. Moroder, T., Gühne, O., Beaudry, N., Piani, M. & Lütkenhaus, N. Entanglement verification with realistic measurement devices via squashing operations. *Phys. Rev. A* **81,** 052342 (2010).
34. Lydersen, L. *et al.* Superlinear threshold detectors in quantum cryptography. *Phys. Rev. A* **84,** 032320 (2011).
35. Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C. & Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2,** 349 (2011).

Acknowledgements

We thank M.A. Broome for assistance with the experimental preparations. We acknowledge financial support from the ARC Discovery and Federation Fellow programs and an IARPA-funded US Army Research Office contract. This research was conducted by the Australian Research Council Centres of Excellence for Engineered Quantum Systems (Project number CE110001013) and Quantum Computation and Communication Technology (Project number CE110001027). The NIST contribution was supported by the NIST Quantum Information Initiative, and is a work of the US Government and as such this article is not subject to US Copyright.

Author contributions

D.H.S., G.G., M.P.de A., T.J.W. and A.F. conducted the experiment and together with A.G.W. designed the experiment and analysed the data. C.B. and H.M.W. developed the theory, and A.L., B.C., T.G., and S.W.N. developed the transition-edge sensors. S.W.N., D.H.S., G.G., M.P.de A. and T.J.W. installed the detectors in the experiment. The manuscript was jointly written by the authors.

Additional information

Competing financial interests: The authors declare no competing financial interests.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

How to cite this article: Smith, D. H. *et al.* Conclusive quantum steering with superconducting transition-edge sensors. *Nat. Commun.* 3:625 doi: 10.1038/ncomms1628 (2012).