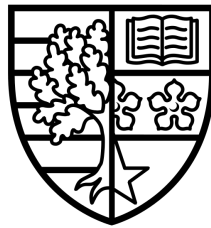


Quantum Networking with Optimised Parametric Down-Conversion Sources

Alexander James Pickston

Submitted for the degree of
Doctor of Philosophy

Heriot-Watt University



Department of Physics
School of Engineering and Physical Sciences

March 2022

The copyright in this thesis is owned by the author. Any quotation from the thesis or use of any of the information contained in it must acknowledge this thesis as the source of the quotation or information.

Abstract

Quantum information processing exploits superposition and entanglement to enable tasks in computation, communication and sensing that are classically inconceivable. Photonics is a leading platform for quantum information processing owing to the relative ease in which the encoding and manipulation of quantum information can be achieved, but there are a set of characteristics that photons themselves must exhibit in order to be useful. The ideal photon source for building up multi-qubit states needs to produce indistinguishable photons with high efficiency. Indistinguishability is crucial for minimising errors in two-photon interference, central to building larger states, while high heralding rates will be needed to overcome unfavourable loss scaling. Domain engineering in parametric down-conversion sources negates the need for lossy spectral filtering allowing one to satisfy these conditions inherently within the source design.

Contained in this Thesis are two experimental investigations. Within the first investigation, we present a telecom-wavelength parametric down-conversion photon source that operates on the achievable limit of domain engineering. The source is capable of generating photons from independent sources which achieve two-photon interference visibilities of up to $98.6 \pm 1.1\%$ without narrow-band filtering. As a consequence, we can reach net heralding efficiencies of 67.5%, corresponding to collection efficiencies exceeding 90%. These sources enable us to efficiently generate multi-photon graph states, constituting the second experimental investigation.

Graph states, and their underlying formalism, have been shown to be a valuable resource in quantum information processing. The generation and distribution of a 6-photon graph state—defining the topology of a quantum network—allows us to explore prospective issues with networks that invoke protocols beyond end-to-end primitives, where users only require local operations and projective measurements. In the case where multiple users wish to establish a common key for conference communication, our proof-of-principle experiment concludes that employing N-user key distribution methods over 2-user methods, results in a 2.13 ± 0.06 key rate advantage.

To my family, and to Laurie.

Acknowledgements

It is hard to believe that four years of my Ph.D. have come to an end. I remember being unsure on what my future was after my undergraduate degree, that was before Alessandro invited me to his lab to show me around before starting a summer project in 2016. As I look back I know for certain that this experience would not have been the same without everyone I have met and worked with over these years. I would therefore like to thank all of you for making my Ph.D. So firstly, I would like to thank Alessandro for his enthusiasm, guidance, help and company at all points of my Ph.D. Your supervision went beyond science, as our discussions would wander from experiments onto test match cricket. You were always available and you always knew exactly what to say to me whenever we discussed anything to re-affirm any confidence that would often waver during my Ph.D. Francesco mentioned in his thesis that your advice to him was to always double-check the email recipients of an email chain after the slip-up you had with an editor. Well I feel that maybe you should have heeded your own advice; I am sure Heriot-Watt's landscaping department would have appreciated that before you demand they pay the processing fee for paper submission. Then, if we continue in temporal order, we arrive at Dmytro. I will always remember the first HOM scan we successfully performed at 4pm on a Friday with the Standa device, giving us measurements in units of revolutions of thread and hastily writing down these horrible units so we remembered where to look Monday, and the cognac you awarded me for being Standa hole punching champion. Francesco, the first of the two Romans, who was more like a mentor initially than a colleague, aiding me with everything from experimental techniques to convincing me to learn Mathematica. Your your willingness to help me with

calculations was unquestionable, and you helped shape my research. The ability you possess, to increase any heralding efficiency I had locally maximised by at least another percent, left me in envy. Peter, for you I have an admission, when we discuss in-depth computing concepts, I understood only the first 5% of things you tell me.

The music you ran through my cars audio system on our road trip to Birmingham will not be forgotten. Mash, the second Roman, who taught me only the finest and most useful Italian words. We went through a lot, the emotional HOM dips we sat at the bottom of tough and the suspected espionage consumed us both for weeks. Chris, your expletive greetings upon arrival into a room I was in and supreme knowledge are just a few of the many things that meant you were a great addition to our group, it was just a shame you occasionally was stuck the wrong side of the curtain. Joseph, in the latter years of my Ph.D you answered

every question I could throw at you and allowed me to gain a much, much deeper understanding of many critical aspects of quantum information processing. I hope we have many more projects to work on together. Andrés and Jonathan, we did not get much time together owing to lockdown, but when we have been together, even though going through the most stressful experiment I have performed, I have enjoyed our discussions. I admire your ambitions for the future of the lab and look forward to seeing you both operating G.34. Berke, our mathematical modelling paper may not have received an official grade, but we both know that Nature are desperate to lay their hands on that manuscript. Lockdown meant that we no longer sat next to each-other, it was not the same without you there. Neil, sorry we took over your office, but at the same time I feel that you enjoyed our company.



Figure 1: The most infamous member of EMQLab, sharpening his theoretical toolset. I have also heard there is a generous award for anyone who can find Mash's bracelet.

My family, whenever I needed a break, and whenever I visited you, you would do everything you could to make sure that I was relaxed. I hope you all know that you supported me in ways that only a wonderful family could.

Finally, I would like to extend my deepest gratitude to Laurie. Whenever I was down you lifted me up, when I was stressed you unflustered me. You kept me sane, you kept me motivated, you are precious.

Research Thesis Submission

Please note this form should be bound into the submitted thesis.

Name:	Alexander James Pickston		
School:	School of Engineering and Physical Sciences		
Version: <i>(i.e. First, Resubmission, Final)</i>	Final	Degree Sought:	Doctor of Philosophy

Declaration

In accordance with the appropriate regulations I hereby submit my thesis and I declare that:

1. The thesis embodies the results of my own work and has been composed by myself
2. Where appropriate, I have made acknowledgement of the work of others
3. The thesis is the correct version for submission and is the same version as any electronic versions submitted*.
4. My thesis for the award referred to, deposited in the Heriot-Watt University Library, should be made available for loan or photocopying and be available via the Institutional Repository, subject to such conditions as the Librarian may require
5. I understand that as a student of the University I am required to abide by the Regulations of the University and to conform to its discipline.
6. I confirm that the thesis has been verified against plagiarism via an approved plagiarism detection application e.g. Turnitin.

ONLY for submissions including published works

Please note you are only required to complete the Inclusion of Published Works Form (page 2) if your thesis contains published works)

7. Where the thesis contains published outputs under Regulation 6 (9.1.2) or Regulation 43 (9) these are accompanied by a critical review which accurately describes my contribution to the research and, for multi-author outputs, a signed declaration indicating the contribution of each author (complete)
8. Inclusion of published outputs under Regulation 6 (9.1.2) or Regulation 43 (9) shall not constitute plagiarism.

* Please note that it is the responsibility of the candidate to ensure that the correct version of the thesis is submitted.

Signature of Candidate:	<i>Alexander James Pickston</i>	Date:	01/03/2022
-------------------------	---------------------------------	-------	------------

Submission

Submitted By <i>(name in capitals)</i> :	Alexander James Pickston
Signature of Individual Submitting:	<i>Alexander James Pickston</i>
Date Submitted:	01/03/2022

For Completion in the Student Service Centre (SSC)

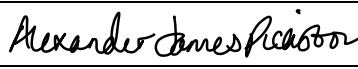
Limited Access	Requested	Yes	No	Approved	Yes	No
<i>E-thesis Submitted (mandatory for final theses)</i>						
Received in the SSC by <i>(name in capitals)</i> :				Date:		


Inclusion of Published Works


Please note you are only required to complete the Inclusion of Published Works Form if your thesis contains published works under Regulation 6 (9.1.2)

Declaration

This thesis contains one or more multi-author published works. In accordance with Regulation 6 (9.1.2) I hereby declare that the contributions of each author to these publications is as follows:

Citation details	A. Pickston , F. Graffitti, P. Barrow, C L. Morrison J. Ho, A G. Brańczyk and Alessandro Fedrizzi, “ <i>Optimised domain-engineered crystals for pure telecom photon sources</i> ”, Optics Express Vol. 29, Issue 5, pp. 6991-7002 (2021)
Author 1, 2, 3, 4, 5, 6	Collected data, analysed data and aided in writing the manuscript.
Author 1, 2	Designed and performed the experiment.
Author 1, 2, 7	Conceived the project, wrote the manuscript.
Signature:	
Date:	01/03/2022

Citation details	F. Graffitti, P. Barrow, A. Pickston , A. M. Brańczyk and Alessandro Fedrizzi, “ <i>Direct Generation of Tailored Pulse-Mode Entanglement</i> ”, Physical Review Letters 124 , 053603 (2020)
Authors 1, 2, 3	Designed and performed the experiment, collected and analysed the data, wrote the manuscript.
Author 4	Provided theoretical support, wrote the manuscript.
Authors 1,5	Conceived the project, wrote the manuscript.
Signature:	
Date:	01/03/2022

Citation details	F. Graffitti, A. Pickston , P. Barrow, M. Proietti, D. Kundys, D. Rosset, M. Ringbauer and Alessandro Fedrizzi “ <i>Measurement Device-Independent Verification of Quantum Channels</i> ” Physical Review Letters 124 , 010503 (2020)
Author 1, 2, 3, 4, 6, 7	Designed and performed the experiment, collected and analysed the data, wrote the manuscript.
Author 6	Aided in theoretical aspects of the work.
Author 1, 2, 5, 6, 7, 8	Wrote the manuscript.
Author 7, 8	Conceived the project.
Signature:	
Date:	01/03/2022

Please included additional citations as required.

Contents

Publications	xi
Publications contained in this thesis	xi
Publications not contained in this thesis	xii
Conference talks and poster presentations	xiii
Preface	xiv
Thesis outline	xv
1 Introduction	1
1.1 Introduction	2
1.2 Quantum information primitives	7
1.3 Stabiliser formalism	10
1.3.1 Graph states	13
1.3.1.1 Local complementation	14
1.4 Circuit model notation	16
1.5 Two-photon interference	17
1.5.1 General two-photon interference	17
1.5.2 Independent Hong-Ou-Mandel interference	19
1.5.2.1 Purity and visibility	21
2 A Source of Photons	23
2.1 Parametric Down Conversion	24

2.1.1	Generating PDC photons	24
2.1.1.1	Departing from a Classical Approach	28
2.2	Down-converted Photon Spectra	31
2.2.1	Pump Envelope Function	32
2.2.2	Phase-matching Function	33
2.2.3	Joint Spectral Amplitude	36
2.2.3.1	Factorisation of the Joint Spectra	37
2.3	Photon Number Statistics	39
2.3.1	Modelling Photon Rates	39
2.3.2	Heralding and Brightness	42
2.4	Concluding remarks	43
3	Photon source for multi-photon state generation	44
3.1	Optimised photon source	45
3.1.1	Source design	46
3.1.2	Domain engineering	48
3.1.2.1	Obtaining a Gaussian PMF	49
3.1.3	Tracking algorithm for domain engineering	52
3.1.4	Focusing conditions	54
3.2	Experimental analysis of source performance	55
3.2.1	Source preparation	56
3.2.2	Independent Hong-Ou-Mandel	58
3.2.3	Reconstructing the Joint Spectrum	62
3.2.3.1	Elongation of Joint Spectrum	65
3.3	Concluding remarks	65
3.3.1	Acknowledgements	66
4	Generating Multi-partite Entanglement	67
4.1	Entangled photon sources	68
4.1.1	Sagnac interferometer	69
4.1.1.1	Note on optical alignment	72
4.2	Linear optical fusion gates	73

4.2.1	Type-I fusion gate	74
4.2.2	Type-II fusion gate	74
4.2.3	Fusion transformations	76
4.2.4	Operating linear optical fusion gates	77
4.3	Concluding remarks	79
5	Photonic Graph States for Quantum Networks	80
5.1	Key distribution within a network	82
5.1.1	Quantum key distribution	82
5.1.2	Conference key agreement	84
5.1.2.1	Asymptotic key rate comparison	86
5.2	Experimental Network Communication	87
5.2.1	Generating an Optical Graph State	89
5.2.2	Transforming into an Optical Graph State	91
5.2.2.1	Distilling states	92
5.2.3	Experimental Preparation of State	95
5.2.4	Experimental verification of state	98
5.2.4.1	Flipped wave-plates	101
5.2.5	Obtaining desired state	103
5.2.5.1	LC operations	104
5.2.5.2	AKR	108
5.3	Concluding remarks	109
5.3.1	Acknowledgements	111
6	Conclusion	112
	Measurement-device-independent verification of quantum chan- nels	117
	Direct generation of pulsed-mode entanglement	124

Publications

Publications contained in this thesis

Alexander Pickston, Francesco Graffitti, Peter Barrow, Christopher L. Morrison, Joseph Ho, Agata M. Brańczyk and Alessandro Fedrizzi, “*Optimised domain-engineered crystals for pure telecom photon sources*”, Optics Express Vol. 29, Issue 5, pp. 6991-7002 (2021).

Francesco Graffitti, Alexander Pickston, Peter Barrow, Massimiliano Proietti, Dmytro Kundys, Denis Rosset, Martin Ringbauer and Alessandro Fedrizzi, “*Measurement Device-Independent Verification of Quantum Channels*”, Physical Review Letters 124, 010503 (2020).

Francesco Graffitti, Peter Barrow, Alexander Pickston, Agata M. Brańczyk and Alessandro Fedrizzi, “*Direct Generation of Tailored Pulse-Mode Entanglement*”, Physical Review Letters 124, 053603 (2020).

Alexander Pickston, Jonathan Webb, Christopher Morrison, Andrés Ulibarrena, Massimiliano Proietti, Joseph Ho and Alessandro Fedrizzi “*Network resource state for efficient conference key agreement*”, In preparation (2022).

Publications not contained in this thesis

Joseph Ho, George Moreno, Samuraí Brito, Francesco Graffitti, Christopher L Morrison, Ranieri Nery, **Alexander Pickston**, Massimiliano Proietti, Rafael Rabelo, Alessandro Fedrizzi and Rafael Chaves, “*Quantum communication complexity beyond Bell nonlocality*”, arXiv preprint arXiv:2106.06552 (2021).

Massimiliano Proietti, Martin Ringbauer, Francesco Graffitti, **Alexander Pickston**, Peter Barrow, Dmytro Kundys, Daniel Cavalcanti, Leandro Aolita, Rafael Chaves, Alessandro Fedrizzi, “*Enhanced multiqubit phase estimation in noisy environments by local encoding*”, Physical review letters 123 (18), 180503 (2019).

Massimiliano Proietti, **Alexander Pickston**, Francesco Graffitti, Peter Barrow, Dmytro Kundys, Cyril Branciard, Martin Ringbauer and Alessandro Fedrizzi “*Experimental test of local observer independence*”, Science advances 5 (9), eaaw9832 (2019).

Farid Shahandeh, Martin Ringbauer, Massimiliano Proietti, Fabio Costa, Austin P Lund, Francesco Graffitti, Peter Barrow, **Alexander Pickston**, Dmytro Kundys, Timothy C Ralph and Alessandro Fedrizzi, “*Assisted Macroscopic Quantumness*”, arXiv preprint arXiv:1711.10498 (2017).

Conference talks and poster presentations

Optimised parametric down-conversion sources for generating telecom graph states, Poster presentation, BQIT, Virtual, (2021).

Winner of the best experimental poster prize.

Quantum memory verification with minimal assumptions, Talk, Photon 18, Birmingham (2018).

Quantum memory verification with minimal assumptions, Talk, Qtech, Edinburgh (2018).

Experimental rejection of observer-independence in the quantum world, Talk, QUISCO meeting, Edinburgh, (2019).

Pure photon generation from domain engineered crystals, Poster presentation, Single Photon Workshop (SPW), Milan, (2019).

Preface

Unexpected things happen, but as much as humanity probably should have been expecting a global pandemic, not many people could have convinced me that as of the 26th of March 2020 we would enter into a national lockdown. Falling almost exactly between elements of work contained in this thesis, the spreading of COVID-19 prompted the shut down of all of our experimental research. The first piece of experimental research that was led by myself, was finalised just before lockdown began, meaning the manuscript for my first, first authored research could be written, re-written and re-written again. But this time also enabled some lab down-time to plan what experiments we can perform next. Initially, planning began on an ambitious multi-photon experiment. After starting our preparations towards the this experiment, it was clear that we just did not have enough of the required resources meaning that this experiment was out of our reach in the near-term. Replacing this experiment however was an experiment that felt almost equally as out of reach at some points.

The pandemic was not alone in being an important date that was defined within the timeline of this thesis, the other important dates—more relevant to the topics of this thesis—were the first demonstrations of a quantum computational advantage. In particular, it was exciting to see quantum computational advantage was achieved using photons generated with probabilistic photon sources based on parametric down-conversion very similar to those displayed in this thesis.

This thesis then, I hope, forms an elegant story beginning with foundational aspects of photon generation and ending with multi-photon state generation as a resource for future quantum network protocols.

Thesis outline

Chapter 1 introduces the work contained in this thesis. We will cover content necessary for comprehending how this thesis adds value to the field of quantum information processing and will touch on the major themes preparing the reader for what is to come. Section 1.1 then introduces some of the fundamental aspects of quantum information that appear in this thesis. There is no new insight in this chapter, but it does contain important theoretical background for subsequent chapters, in particular the stabiliser formalism and graph states.

Chapter 2 introduces the fundamental aspects of parametric down-conversion and we go through how, starting from some fundamental equations in optics, we can arrive at a quantum state describing down-conversion.

Chapter 3 goes into some more detail into down-conversion, specifically on how one can achieve spectrally pure photons from photon source engineering alone. This chapter culminates in an experimental analysis of the subsequently designed crystal. As a result of this work, we can explore multi-photon tasks. But before we introduce a full scale application, we enter into an intermediary chapter.

Chapter 4 outlines how one produces multi-photon entangled states with parametric down-conversion sources, introducing the optical arrangement we use in our experimental lab to generate Bell states with high purity and sufficient rates. We also introduce fusion gates, the experimental aspects behind them and how these gates generate larger multi-photon states.

Chapter 5 contains the final work in this thesis and also the final work of my PhD. Genuine multi-photon entanglement can be a very powerful resource for quantum networks. We go beyond typical scenarios which distribute GHZ states and Bell states directly, and produce a genuine multi-partite entangled network resource state. The generated states equivalence to a graph allows access to a toolbox of local operations (single qubit unitaries) such that in one network usage, users can distill a GHZ between a subset of users, or a Bell state between several subsets of users without requiring them to perform non-local operations. Our analysis con-

cludes with measurements of the asymptotic key rate for a GHZ state and set of Bell states, highlighting the advantage of N-user quantum key distribution over 2-user quantum key distribution key rate.

Chapter 6 concludes this thesis, by restating the key points of this thesis and relating the importance of this work with respect to current research directions in quantum information processing.

Chapter 1

Introduction

1.1	Introduction	2
1.2	Quantum information primitives	7
1.3	Stabiliser formalism	10
1.3.1	Graph states	13
1.3.1.1	Local complementation	14
1.4	Circuit model notation	16
1.5	Two-photon interference	17
1.5.1	General two-photon interference	17
1.5.2	Independent Hong-Ou-Mandel interference	19
1.5.2.1	Purity and visibility	21

*If computers that you build are quantum,
Then spies of all factions will want 'em.
Our codes will all fail,
And they'll read our email,
Till we've crypto that's quantum, and daunt 'em.*

—Jennifer and Peter Shor

At the intersection of computer science, physics and mathematics lies quantum information processing. Exactly what quantum information processing contains is epitomised quite well by the above limerick. It is the computation, storage and transmission of quantum information.

1.1 Introduction

Much departed from classical information, where information is encoded in logical bits assigned to definite values, an elementary unit of quantum information is analog meaning a qubit can exist as a coherent superposition of basis states. Further, we cannot discriminate with certainty between quantum states that are non-orthogonal nor can one measure or copy the state without disturbing it. The most remarkable property of quantum information though, is that quantum systems can be entangled. A consequence of entanglement—characteristic correlations with no classical counterpart—is to try to isolate properties of an individual system constituting part of an entangled system is ill-fated. Entanglement was at the heart of the illustrious philosophical debate probing the nature of reality, concerned with whether quantum theory could be considered complete. In the so-called EPR paper, named after the authors A. Einstein, B. Podolsky and N. Rosen, it was postulated that a complete

physical theory must satisfy local realism, and thus quantum theory should be extended to encompass hidden variables [1]. The debate over whether these hidden variables had a place in quantum theory was ended in 1964 when J. S. Bell derived the famed inequality, and the designation of a “Bell state” was to be reserved to quantum systems that were maximally entangled [2].

Quantum theory may have emanated in the early 20th century, but it was not until the later half of the 20th century that the theory began to facilitate some of the most influential experimental and theoretical research, formally establishing the field of quantum technology. Of these quantum technological tasks, quantum communication—at the time of its theoretical proposal—was the most experimentally feasible. The origins this technology is a fascinating story that is re-called in detail within Ref. [3]. Briefly, the first account of employing quantum theory for the purpose of security was in the early 70s but only appeared in print in the early 80s, where S. Wiesner postulated unforgeable bank notes [4]. It took a conversation on a beach before a paper was published that explicitly contained the term “Quantum Cryptography” [5], where the authors toyed with the idea of using photons as quantum information carriers stored on unforgeable subway tokens. Shrewdly, C. H. Bennet and G. Brassard observed that

“God did not create photons as a storage medium, but rather
as a communications device” [6],

birthing the renowned “BB84” protocol [7] and the beginning of almost 40 years of experimental research into quantum key distribution.

Almost simultaneous to early discussions surrounding quantum communication, R. Feynman was indicating that to efficiently simulate quantum systems, we would require quantum computers [8]. Where the promise of quantum communication was security, quantum computation promised exponential speed-ups and the capability to solve tasks that are currently intractable with classical computers. Algorithms—designed for use with quantum computations—can drastically outperform their classical equivalents, some of the most notable algorithms include P. Shor’s prime factoring algorithm [9] and L. Grover’s database search algorithm [10].

There are many physical systems that can be encoded for quantum information

processing, but out of optical systems, trapped ions, silicon spin and cold atoms, optical systems are the most flexible and arguably the easiest to use. Photons can be precisely prepared, coherently controlled, efficiently detected and are free from decoherence from interactions with the environment, meaning optical systems can be deployed for all aspects of quantum information processing: computation, storage and transmission of quantum information. Since the inception of the laser in the 1960s, the quantity of research into photonics dwarfs research into quantum information processing. The maturity of photonics, and the deep understanding of its central topics therefore means that we can leverage the existing technological base of classical photonics.

Pioneering works on the teleportation of a quantum state and the swapping of entanglement are examples of quantum based tasks that employ photonics. The composition of most entanglement based optical quantum information tasks are founded on these pioneering pieces of work. It was in 1993 when C. H. Bennet, G. Brassard and co-authors proposed a “teleporting” scheme that consisted of two users, who defying no physical laws and adhering to well known axiom of no-cloning, wish to exchange all the information about a quantum system without sending the system itself. The now well known quantum teleportation protocol, requires two users to share long-range correlations, owed to the fact that they each possess a bi-partition of a maximally entangled photonic quantum state, a Bell state [11]. One user, who wishes to teleport an unknown quantum state, performs a joint Bell measurement onto their bi-partition and the quantum state for teleportation. The result of the joint measurement—that is communicated classically—dictates which, if any, local unitary is required in a feed-forward step to successfully teleport the unknown state. The first experimental realisation of teleportation was subsequently performed by D. Boschi *et al.* in 1998 [12], using a process called parametric down-conversion to generate the entangled photons required.

In the same year that C. H. Bennet, G. Brassard and co-authors proposed the teleportation of quantum states, M. Żukowski *et al.* proposed the teleportation of entanglement, or what the authors called entanglement swapping. Entanglement swapping, is the entangling of two systems that have never interacted and this oper-

ation can act as a means to distribute entanglement between distant users [13]. Performing a joint Bell measurement on bi-partitions of two different entangled states, leaves the remaining bi-partitions entangled, attaining correlations they never had. This was first demonstrated experimentally by J. W. Pan *et al.* also in 1998 [14], again using the parametric down-conversion process to generate entangled photons.

Both entanglement swapping and teleportation rely on a so called Bell state measurement. This is a projection onto the Bell basis [15] that was translated into an optical scheme by S. L Braunstein and A. Mann in 1995 [16], via the generalisation of Hong-Ou-Mandel interference [17] and depended yet again on the generation of photon pairs using parametric down-conversion.

These proposals and their subsequent experimental realisation, are major precursors for many protocols in optical quantum information science, such as loop-hole free Bell tests [18], Boson sampling [19, 20], ghost imaging [21] and all-optical quantum repeaters [22] (the list goes on). At the very foundation of these tasks—and a resource of most tasks in optical quantum information processing in general—is the generation of entangled photons through parametric down-conversion, a major theme of this thesis.

Parametric down-conversion (PDC) is the most widely used technique for generating entangled photons. It was P. Kwiat *et al.* in 1995 who demonstrated the first efficient source of polarisation entangled photons [23]. As a result of its cost-effectiveness and accessibility, entangled photon generation via PDC has been developed extensively, incorporating countless different optical schemes, accessing a variety of different degrees-of-freedom [24–30] and exhibiting up to twelve-photon entanglement [31–33].

As will be presented in this thesis, we are approaching the upper bound of what is possible with current PDC photon sources in terms of photon distinguishability and photon generation rates. It is exciting to know that as of writing this thesis, most of the intrinsic limitations of PDC have been removed.

Epitomised in the work of Ref. [34]—which deployed probabilistic photon sources very similar to those displayed in this thesis to demonstrate the landmark of “quan-

tum supremacy”¹—multi-photon experiments absolutely need high success two-photon interference. Any reductions in the success probability of two-photon interference can create huge over-heads in terms of the number of photon sources required, subsequently the number of detectors, the complexity of the photonic circuit and the complexity of processing the results [37]. Only indistinguishable—which by definition also means spectrally pure—photons can interfere with a maximum probability of success [38]. As a result, pushing photon sources to the achievable limits of indistinguishability, whilst maintaining suitable generation rates is the focus in the early parts of this thesis.

The later parts then focus on exploiting the near-ideal photon sources we have developed for an investigation into quantum network primitives with photonic graph states. Quantum networks at the desired global scale are still notional, that is, they are not yet of the scale of classical networks. But, there have been many examples of small and intermediate scale networks that have established both the basic infrastructure, as well as more advanced infrastructure required for larger networks, such as satellite links [39–46]. Prospective networks will progress further than just a means for point-to-point communication, where communication can occur simultaneously across the underlying network. The infrastructure of a network and the simultaneity of communication means that certain networks are susceptible to bottlenecks. A solution to this, is to employ genuine multi-partite entanglement in the form of a graph state, and distribute its partitions to network users. This graph forms an underlying resource for the generation of a secure key between multiple users. We highlight experimentally, that a point-to-point distribution of a key for a multi-user communication protocol is inefficient compared to a conference key agreement scheme.

Before entering the main work contained in this thesis, we will discuss key theory tools necessary for the comprehension of the main work.

¹Even though we had only just entered the phase of noisy-intermediate scale quantum (NISQ) computing, “quantum supremacy”, a term coined by Preskill [35], was reported in landmark papers [34, 36].

Quantum Information Processing

The goal for the remaining parts of this chapter is not to introduce the reader to any new physics or concepts unique to this thesis, but to outline some of the fundamental theory contained in the rest of this thesis. There are a multitude of resources that contain a lot of the following information, but the ones I have found most useful and therefore used the most are Refs. [47–51].

1.2 Quantum information primitives

A qubit is a two-level quantum system which can be represented by a vector in a two-dimensional Hilbert space \mathcal{H} . A basis set of this quantum system are two mutually orthogonal normalised vectors. Traditionally, the “computational basis” is expressed as:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (1.1)$$

but within this thesis, the computational basis will take the form of horizontal $|H\rangle$ and vertical $|V\rangle$ polarisation, a result of the encoding space optical systems offer. Quantum states can also exist in a linear superposition of the computational basis,

$$|\psi\rangle = \cos \frac{\theta}{2} |H\rangle + e^{i\phi} \sin \frac{\theta}{2} |V\rangle, \quad (1.2)$$

with the angles θ and ϕ describing the polar and azimuthal angles that map a three-dimensional sphere called the Bloch sphere depicted in Figure (1.1). Lying on the axes of this sphere are the eigenstates of the Pauli operators. Expressed in terms of

polarisation, the states that lie on the x -axis are

$$|D\rangle = \frac{(|H\rangle + |V\rangle)}{\sqrt{2}} \quad \text{and} \quad |A\rangle = \frac{(|H\rangle - |V\rangle)}{\sqrt{2}}, \quad (1.3)$$

whilst the states lying on the y -axis are,

$$|R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle) \quad \text{and} \quad |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle). \quad (1.4)$$

Leaving just the computational basis vectors, which lie on the z -axis. Pauli matrices are incredibly important in quantum mechanics. The 2×2 complex matrices are traceless, hermitian, unitary and have a determinant of minus one. They also have the property that they anti-commute with each-other and their square produces the identity matrix \mathbb{I} . The Pauli group \mathcal{P} , contains the following

$$\sigma_z = \mathbb{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \sigma_x = \mathbb{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \mathbb{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}. \quad (1.5)$$

These operations applied on a single qubit correspond to a bit flip for \mathbb{X} , a phase flip for \mathbb{Z} and a combination of bit and phase flip for \mathbb{Y} . A final crucial operator used frequently in this thesis is the Hadamard gate, which transforms Pauli operators into other Pauli operators under their conjugation. Equivalently, the Hadamard

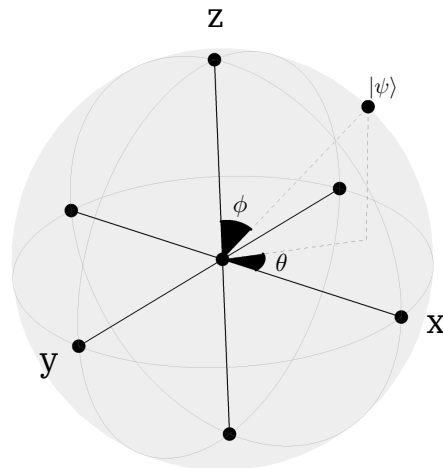


Figure 1.1: The Bloch sphere. This is a geometrical representation of the pure state space of a two-level quantum system. The x, y and z axes intersect the sphere at the eigenstates of the respective Pauli matrices σ_x, σ_y and σ_z .

gate transforms the eigenstates of the Pauli operators, its definition is as follows:

$$\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (1.6)$$

I will just quickly introduce some nomenclature when it comes to the definition of quantum states. Throughout this thesis polarisation encoding is used meaning that we may interchange how we describe states, adhering to the following:

$$|0\rangle \equiv |\mathbf{H}\rangle \quad |1\rangle \equiv |\mathbf{V}\rangle \quad |+\rangle \equiv |\mathbf{D}\rangle \quad |-\rangle \equiv |\mathbf{A}\rangle$$

omitting the eigenstates of \mathbf{Y} which are sparsely used.

Typically we operate within either the state vector form or density operator form. Both of these forms are mathematically equivalent, meaning that we can freely interchange between their usages. In the density operator form we have access to the density operator, which is defined as

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i| \quad (1.7)$$

and can describe quantum systems whose states are not entirely known. The density operator is typically used in the description of pure quantum states. It is trace preserving, positive semi-definite—enforcing its eigenvalues to be non-negative—and is self-adjoint. Mixed states can also be represented in this formalism, where the density matrix of a fully mixed state becomes $\rho = (1/d)\mathbb{I}_d$, where d is the dimension of the state. In such a condition of mixture, the density operator can no longer define a unique state, but instead describes an ensemble of mixed states.

The measure of state purity discriminates between pure and mixed states. The purity is measured by computing:

$$\mathcal{P} = \text{Tr}[\rho^2]. \quad (1.8)$$

Following from the condition of mixture on the density operator, the purity of a mixed state is bound to $1/d \leq \mathcal{P} < 1$, whilst a pure state has purity $\mathcal{P} = 1$.

The fidelity is a distance measure, which determines how close a state is to a desired target state. There are two different definitions of a fidelity measure

depending on whether the states you are calculating against are pure or mixed. For pure states the fidelity is

$$\mathcal{F}(\rho_{\text{target}}, |\psi\rangle) = \langle\psi|\rho_{\text{target}}|\psi\rangle, \quad (1.9)$$

and for mixed states

$$\mathcal{F}(\rho'_{\text{target}}, \rho_{\text{mix}}) = \left(\text{Tr} \left[\sqrt{\rho_{\text{mix}} \rho'_{\text{target}} \rho_{\text{mix}}} \right] \right)^2. \quad (1.10)$$

Measurements in the density operator formalism are analogous to measurements in the state vector approach. So as we mentioned, one can interchange between the two. Consider a set of measurement operators M_m and an initial state $|\psi_i\rangle$. The probability of attaining the result m is

$$p(m) = \sum_i p_i \langle\psi_i| M_m^\dagger M_m |\psi_i\rangle = \text{Tr}[M_m^\dagger M_m \rho]. \quad (1.11)$$

The quantum state after obtaining result m is then

$$\rho_m = \sum_i p_i \frac{M_m |\psi_i\rangle \langle\psi_i| M_m^\dagger}{\text{Tr}[M_m^\dagger M_m \rho]} = \frac{M_m \rho M_m^\dagger}{\text{Tr}[M_m^\dagger M_m \rho]}. \quad (1.12)$$

So far we have only introduced single-qubit states. The most important two-qubit states are the Bell states (or also referred to as EPR pairs). These are maximally entangled pure states that produce correlations from joint measurements that triggered foundational debates within quantum mechanics. They play a fundamental role in quantum information processing and within this thesis, and are thus defined as

$$|\Phi^\pm\rangle = \frac{|\text{HH}\rangle_{12} \pm |\text{VV}\rangle_{12}}{\sqrt{2}},$$

$$|\Psi^\pm\rangle = \frac{|\text{HV}\rangle_{12} \pm |\text{VH}\rangle_{12}}{\sqrt{2}}.$$

1.3 Stabiliser formalism

Descriptions of quantum states and any subsequent transformations applied to those states requires a set of mathematical tools. One such set of tools is the stabiliser formalism, initially conceived by D. Gottesman for the purpose of error correction

codes [52] which now extends beyond its intended first use case. Its mathematical foundation is based on using sets of operators (or an operator depending on the size of Hilbert space that state occupies) to describe both states and the transformations on that state. So rather than describing a pure state as a vector in Hilbert space, we describe the state via a set of operators (or an operator) that obtains the +1 eigenvalue of the eigenstate. For example the eigenstate of \mathbb{Z} is $|\mathbf{H}\rangle$ with corresponding eigenstate of +1, whilst mapping the eigenvalue of $|\mathbf{V}\rangle$ to the operator \mathbb{Z} requires a minus sign. The same for the \mathbb{X} operator, which has eigenstate $|\mathbf{D}\rangle$ with eigenvalue +1 and orthogonal eigenstate $|\mathbf{A}\rangle$ which has an eigenvalue of -1 . We can therefore map the single-qubit states to their respective operators

$$\begin{aligned}\mathbb{Z}|\mathbf{H}\rangle &= |\mathbf{H}\rangle & -\mathbb{Z}|\mathbf{V}\rangle &= |\mathbf{V}\rangle \\ \mathbb{X}|\mathbf{D}\rangle &= |\mathbf{D}\rangle & -\mathbb{X}|\mathbf{A}\rangle &= |\mathbf{A}\rangle.\end{aligned}\tag{1.13}$$

Beyond the single-qubit case, we can also consider how this formalism can be used to describe the Bell state $|\Phi^+\rangle$. This state can be described by two sets of operators $\mathbb{Z}_1\mathbb{Z}_2$ and $\mathbb{X}_1\mathbb{X}_2$ as the following relation adheres to the formalism:

$$\begin{aligned}\mathbb{Z}_1\mathbb{Z}_2\left(\frac{|\mathbf{HH}\rangle_{12} + |\mathbf{VV}\rangle_{12}}{\sqrt{2}}\right) &= \left(\frac{|\mathbf{HH}\rangle_{12} + |\mathbf{VV}\rangle_{12}}{\sqrt{2}}\right) \\ \mathbb{X}_1\mathbb{X}_2\left(\frac{|\mathbf{HH}\rangle_{12} + |\mathbf{VV}\rangle_{12}}{\sqrt{2}}\right) &= \left(\frac{|\mathbf{HH}\rangle_{12} + |\mathbf{VV}\rangle_{12}}{\sqrt{2}}\right).\end{aligned}\tag{1.14}$$

More generally, the collection of operators that describe the state are known as the “stabilizer” of the state. If $|\psi\rangle$ is the quantum state, then a stabilizer is a set of operators S_i that leave the state invariant

$$S_i|\psi\rangle = |\psi\rangle.\tag{1.15}$$

The group that can describe all of the operators in the stabilizer formalism is the Pauli group \mathcal{P}_n for n qubits. For one qubit the Pauli group is composed of the product of the Pauli matrices with ± 1 and $\pm i$,

$$\mathcal{P}_1 = \{\pm i; \pm 1\} \times \{\mathbf{I}, \mathbf{Z}, \mathbf{X}, \mathbf{Y}\},\tag{1.16}$$

and the Pauli group for n -qubits is defined by the tensor product of n Pauli groups

$$\mathcal{P}_n = \mathcal{P}_1^{\otimes n}. \quad (1.17)$$

For a particular quantum state $|\psi\rangle$ we can describe the stabilizer group \mathcal{S} , whereby each element of this group stabilizes the state. By way of definition, only commuting operators can have simultaneous eigenvectors, meaning that the group of stabilizers \mathcal{S} is Abelian.

Consider that two operators, S_i and S_j individually stabilize $|\psi\rangle$, their unique products $S_i S_j$ and $S_j S_i$ will also stabilize $|\psi\rangle$. This means that $S_i S_j$ and $S_j S_i$ form two new stabilisers S_k and S_l satisfying $S_i S_j |\psi\rangle = S_k |\psi\rangle = |\psi\rangle$ and $S_j S_i |\psi\rangle = S_l |\psi\rangle = |\psi\rangle$ respectively. We can reduce the stabilizer group \mathcal{S} into its “generators” \mathcal{G} , which are the smallest set of independent elements that can be used to produce all the other elements belonging to that group [47]. Explicitly then, the full group of stabilizers \mathcal{S} can be obtained with just the sub-group of m generators $\mathcal{G} = \langle S_1, \dots, S_m \rangle$.

Rather than tracking the evolution of a state in time under unitary transformations, within the stabilizer formalism states are fixed and operators are evolved in time such that information processing is described by operator transformation rules alone. Both of these aspects mean we are working within the Heisenberg picture of quantum mechanics, opposed to the Schrödinger picture. The application of a unitary transformation to a quantum state in these mathematical frameworks corresponds to the following mapping:

$$\text{Schrödinger: } |\psi\rangle \xrightarrow{\hat{U}} |\psi'\rangle = \hat{U} |\psi\rangle \quad (1.18)$$

$$\text{Heisenberg: } \langle S_i \rangle \xrightarrow{\hat{U}} \langle S'_i \rangle = \hat{U} S_i \hat{U}^\dagger \quad (1.19)$$

Only a sub-class of all possible quantum operations can be described within the stabilizer formalism, that is operations which transform a Pauli product into another Pauli product under its conjugation. Such transformations are classed as Clifford operations, where under such an operation, the evolution of a quantum state in the stabilizer formalism is a mapping of the generators according to $S_m \rightarrow \hat{U}_C S_m \hat{U}_C^\dagger$ where $S_m \in \mathcal{G}$. The evolution is now equivalent to finding the new unique generators that stabilize the new rotated state. This creates a favourable scaling in the number

of bits required to store a full quantum state [53]. Generators of the Clifford set are the CNOT, Hadamard, and phase gate.

The importance of this formalism beyond the context of error correction, is discussed later in this thesis, but a more critical discussion for this thesis revolves around the strict criteria for what states this formalism can be used for. Only states that are stabilised by Pauli operations (stabiliser states) can be used and within this restricted set of states. A sub-group of the stabiliser states, known as graph states, are frequently discussed towards the end of this thesis, after we have introduced multi-photon state generation. It is useful to form an understanding of the structure of these states and how they can be manipulated with simple single-qubit operations and measurements.

1.3.1 Graph states

A graph state is an n -qubit stabiliser state. Their correspondence to an n -vertex mathematical graph makes them a very useful tool in photonic quantum information processing. All stabiliser states are locally equivalent to a graph state [54], which consist of edges E connecting n vertices V . Explicitly a graph $G = (V, E)$ is defined as

$$|G\rangle = \prod_{i,j \in E} CZ_{ij} |+\rangle^{\otimes |V|}, \quad (1.20)$$

where an edge between two vertices corresponds to a non-local gate ($CZ = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|$) applied onto the two vertices the edge connects, and each vertex is a single-qubit prepared as $|+\rangle$). Interestingly, in the stabilizer framework, before applying the CZ operations, each vertex is initially in the state $|+\rangle$ which is stabilized by X , meaning the generator of the state $|+\rangle_n$ would simply be the list $\langle X_1, X_2, \dots, X_n \rangle$.

A property of graphs that we exploit in Chapter 5 is that different graphs, which may be constructed in vastly different ways, with different entanglement structure, can be locally equivalent up to Clifford operations [55], where transforming from one graph into another is achieved by performing a graph operation called local complementation (LC).

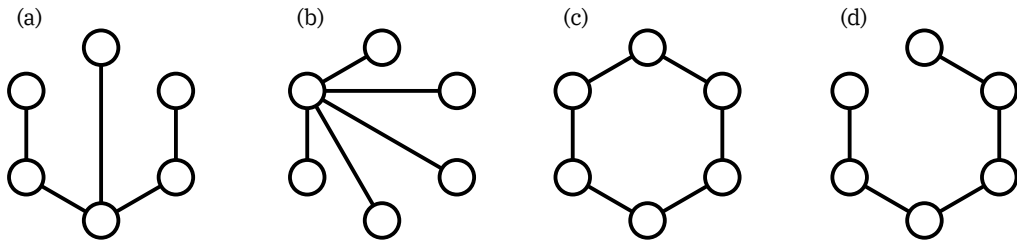


Figure 1.2: A small collection of 6-qubit graph states. Each of the graphs in this collection are not LC equivalent, meaning that they each exist in a distinct “orbit”. An interesting property of graph (b) is that it is LU equivalent to the GHZ state, up to Hadamard rotation on its leaf-nodes (vertices that are adjacent to precisely one other vertex). The properties of graphs becomes extremely interesting when considering certain network protocols. Later on in this thesis we exploit the properties of (a).

1.3.1.1 Local complementation

Local complementation is an equivalent action to the application of a set of local Clifford gates [54]. Starting with an initial graph $|G(V, E)\rangle$ the LC operation applies:

$$U_t^{\text{LC}} |G\rangle = |\text{LC}_t(G(V, E))\rangle = |G(V, E')\rangle, \quad (1.21)$$

altering the structure of the graph. Graphically, application of local complementation LC_t , on a vertex $t \in V$, complements the neighbourhood of vertex $N(t) \in V$. This constitutes locating the neighbouring vertices of t , removing their edges (if they have any edges), and adding edges that were not initially present, leaving the graph transformed $G = (V, E')$. Figure (1.3) shows the action of the LC onto a graph.

An important point regarding graph transformations and LC is that graphs that are equivalent under local Clifford unitaries are not necessarily equivalent under local unitary (LU) operations [56]. Repeated application of LC operation on differ-

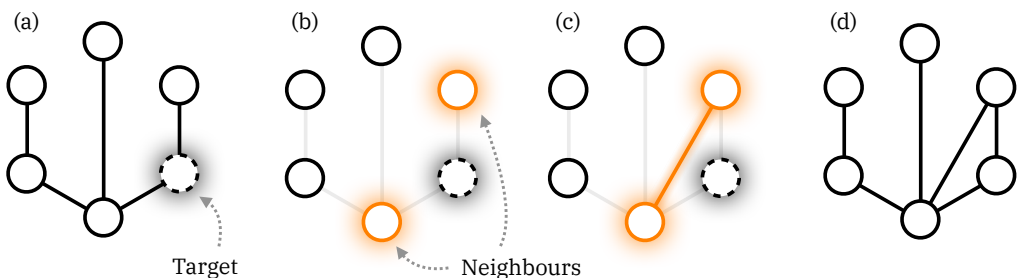


Figure 1.3: Local complementation. Transforming an initial graph state (a) via local complementation applied to a target qubit—highlighted as the dashed vertex—conforms to the following. The neighbourhood sub-graph (b) of the target qubit is complemented by removing the existing edges, and adding edges that were not present (c). Then, all the initial edges are added back to obtain the LC equivalent graph (d).

ent vertices of an initial graph allows one to explore the associated “orbit” of that graph. This “exploration” contains all graphs that exist in the same class of entanglement [55, 57]. Interestingly, this “orbit” can also be represented by a graph [57]. Graphs with the same structure but alternate vertex labelling are isomorphic, meaning they sit within the same orbit and thus the same entanglement class. The following definite local operation implements the complementation [54, 55, 57]:

$$U_t^{\text{LC}} = \sqrt{-i\mathbb{X}_t} \bigotimes_{v \in N(t)} \sqrt{-i\mathbb{Z}_v} \quad (1.22)$$

where t denotes the target vertex and v denotes the set of neighbouring vertices to the target $N(t)$.

Performing single-qubit measurements on a graph alters the structure of the graph. Measurements in the \mathbb{Z} basis removes the vertex being measured and its corresponding edges. A measurement in the \mathbb{Y} basis consists of a \mathbb{Z} basis measurement on the complemented graph. Both of these are shown in Figure (1.4). Measurements in the \mathbb{X} basis are slightly more complicated, and not used within this thesis. It requires a random choice of vertex that neighbours the target. A LC operation is applied to this neighbouring vertex on a temporary basis, a \mathbb{Y} measurement is performed on the target vertex, and finally, the LC operation is undone.

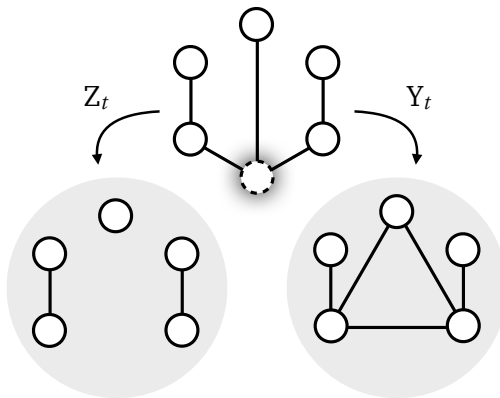


Figure 1.4: Measurements on Graphs. A measurement in the \mathbb{Z} basis, shown on the left hand side of removes the vertex being measured along with its edges. Measurements in the \mathbb{Y} basis, shown on the right, consists of a \mathbb{Z} basis measurement on the complemented graph.

1.4 Circuit model notation

As a result of the definition of a graph state, the circuit model equivalent of the graph is very easy and intuitive to arrive at. Every vertex of the graph translates into the initialisation of a qubit in the $|+\rangle$ state, every edge is represented by a CZ gate. Once one has the circuit equivalent of a graph, the generators of the state can also be discovered easily through inspection of the circuit. Another benefit of the circuit notation is the fact one could implement theoretical investigations on the state with a variety of different open source platforms containing toolboxes for implementing quantum operations such as Qiskit [58].

In Chapter 5, we explicitly use the circuit equivalent of a specific graph, along with a number of local operations applied to each qubit to determine exactly how to obtain measurement settings with correct operations encoded onto them. Figure (1.5) shows useful circuit notation concepts. Careful considerations are required when using circuit equivalent of a Bell state or GHZ states, ensuring that Hadamard rotations are not omitted.

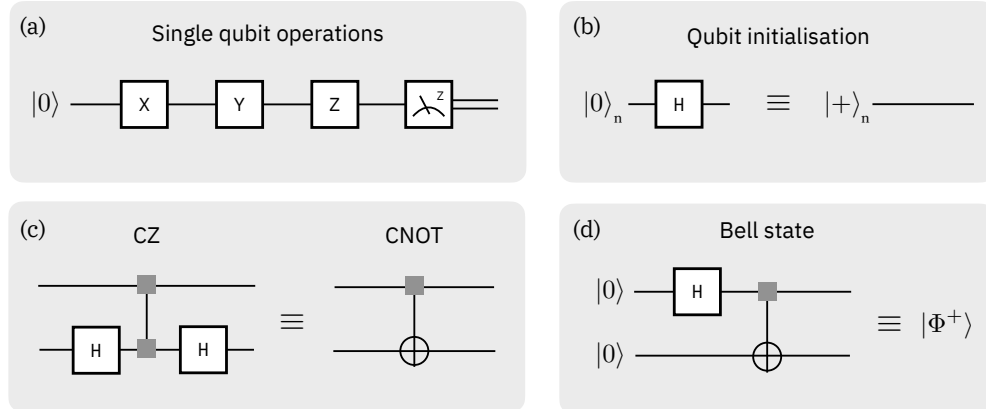


Figure 1.5: Useful circuit notation. Each rail represents a qubit initialised in a specific state, typically the ground state of the computational basis. The qubit in (a) is rotated by single qubit Pauli gates followed by a measurement in the computational basis, represented by the small Z . The two rails after the measurement represent classical information. Initialisation of a qubit does not have to be in the computational basis. Rotating from the computational basis into the X basis requires a Hadamard rotation, (b) shows the equivalence. Non-local gates represent the interaction of two qubits, and are non-trace preserving operations. The most common two-qubit gates are the CZ and CNOT, (c) highlights how to represent a CNOT in terms of CZs, a useful tool when working with graph states. Finally, we show the simple circuit formalism for representing a Bell state (d).

1.5 Two-photon interference

There is an essential reliance throughout this thesis on the mechanism typically called Hong-Ou-Mandel (HOM) interference, named after the authors who experimentally verified the effect [17]. The premise of HOM interference is the effects of two indistinguishable photons interacting on a beam splitter (BS). In this section we introduce some essential notation for describing joint photon spectrum—more detail of which is provided in latter chapters where we focus on photon sources—as well as explicitly derive the results from two-photon interference. Although the derivation is well understood and simple, its importance is particularly prevalent considering that it is a very accessible way to benchmark the performance of a photon source.

1.5.1 General two-photon interference

To derive the interesting results that explain how one can use two-photon interference to characterise photons, we must first consider the most general case, whereby two photons are incident on a 50:50 beam splitter:

$$\hat{a}^\dagger \hat{b}^\dagger |0, 0\rangle_{ab} = |1, 1\rangle_{ab} \quad (1.23)$$

where \hat{a}^\dagger and \hat{b}^\dagger are creation operators that act on vacuum creating single photons each in a well defined spatial mode. The two spatial modes, a and b , are the inputs of the BS, whilst the two output spatial modes are also noted as a and b , see Figure (1.7)(a). The transformation imposed onto the creation operators in the input mode, considering that the BS is 50:50, creates photons in the output modes according to:

$$\hat{a}^\dagger \xrightarrow{\hat{U}_{BS}} \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{b}^\dagger), \quad (1.24)$$

$$\hat{b}^\dagger \xrightarrow{\hat{U}_{BS}} \frac{1}{\sqrt{2}}(\hat{a}^\dagger - \hat{b}^\dagger). \quad (1.25)$$

Calculating the full state after the interaction on the BS, and considering that the input photons are indistinguishable from another leads to the following result:

$$\begin{aligned}
\hat{a}^\dagger \hat{b}^\dagger |0, 0\rangle_{ab} &\longrightarrow \frac{1}{2}(\hat{a}^\dagger + \hat{b}^\dagger)(\hat{a}^\dagger - \hat{b}^\dagger) |0, 0\rangle_{ab} \\
&= \frac{1}{2}(\hat{a}^\dagger \hat{a}^\dagger + \hat{a}^\dagger \hat{b}^\dagger - \hat{a}^\dagger \hat{b}^\dagger - \hat{b}^\dagger \hat{b}^\dagger) |0, 0\rangle_{cd} \\
&= \frac{1}{2}(\hat{a}^\dagger \hat{a}^\dagger |0, 0\rangle_{ab} - \hat{b}^\dagger \hat{b}^\dagger |0, 0\rangle_{ab}) \\
&= \frac{1}{\sqrt{2}}(|2, 0\rangle_{ab} - |0, 2\rangle_{ab}).
\end{aligned} \tag{1.26}$$

In this case, the probability of detecting a single photon in each mode, also referred to as a coincidence count, is $p = 0$.

Now, let us consider two input photons with arbitrary spectral amplitudes defined as ϕ_i centred at a frequency ω_i . Given this, a photon entering the BS in mode a is now defined as:

$$|1, \phi_i\rangle_i = \int d\omega_i \phi_i(\omega_i)_a \hat{a}^\dagger(\omega_i) |0\rangle_a, \tag{1.27}$$

where the spectral amplitude satisfies the condition $\int d\omega |\phi(\omega)|^2 = 1$, and the input two-photon state becomes

$$\begin{aligned}
|\psi^{in}\rangle_{ab} &= |1; \phi_a\rangle_a |1; \phi_b\rangle_b \\
&= \int d\omega_a \phi_a(\omega_a) \hat{a}^\dagger(\omega_a) |0\rangle_a \int d\omega_b \phi_b(\omega_b) \hat{b}^\dagger(\omega_b) e^{-i\omega_b \tau} |0\rangle_b,
\end{aligned} \tag{1.28}$$

where we added a temporal delay in order to introduce distinguishability and account for photon wave-packets that are not overlapped in time. The BS unitary operation on the input two-photon state can now be calculated, skipping the trivial expansion step:

$$\begin{aligned}
|\psi^{out}; \tau\rangle_{cd} &= \hat{U}_{BS} |\psi^{in}; \tau\rangle_{ab} \\
&= \frac{1}{2} \int d\omega_a \phi_a(\omega_a) \int d\omega_b \phi_b(\omega_b) e^{-i\omega_b \tau} (\hat{a}^\dagger(\omega_a) \hat{a}^\dagger(\omega_a) + \hat{a}^\dagger(\omega_a) \hat{b}^\dagger(\omega_b) \\
&\quad - \hat{a}^\dagger(\omega_a) \hat{b}^\dagger(\omega_b) - \hat{b}^\dagger(\omega_b) \hat{b}^\dagger(\omega_b)) |0, 0\rangle_{ab}.
\end{aligned} \tag{1.29}$$

In order to determine the full result of the transformation, we need to define some projectors that represent the detection of a photon in each output mode. The

projector on mode a is,

$$\hat{P}_a = \int d\omega \hat{a}(\omega) |0\rangle_a \langle 0|_a \hat{a}(\omega), \quad (1.30)$$

and an analogous definition for mode b . Using the Born rule the probability of detecting a photon in each output mode, and also therefore equally the probability of detecting a coincidence is given by:

$$p_{cc}(\tau) = \text{Tr}[\rho^{\psi^{out}}; \tau]_{ab} \langle \psi^{out}; \tau |_{ab} \hat{P}_a \otimes \hat{P}_b]. \quad (1.31)$$

Substituting Equations (1.29) and (1.30) with the above, using certain creation/annihilation operator rules and the normalisation condition, we obtain

$$p_{cc}(\tau) = \frac{1}{2} - \frac{1}{2} \int d\omega_a \phi_a^*(\omega_a) \phi_b(\omega_a) e^{-i\omega_a \tau} \int d\omega_b \phi_b^*(\omega_b) \phi_a(\omega_b) e^{-i\omega_b \tau}. \quad (1.32)$$

This equation is important but in order to advance our discussion of two-photon interference we will consider the scenario that the two incident photons are generated by independent sources (or independent generation events).

1.5.2 Independent Hong-Ou-Mandel interference

Otherwise referred to as heralded photon interference, we can now examine what happens when two photons from separate sources interfere on the BS. Moving away from the above generalisation, where we have considered photons that are spectrally pure, we now consider mixed states. For mixed states, the joint photon spectrum is expressed as a statistical mixture of orthogonal modes:

$$f(\omega_1, \omega_2) = \sum_k u_k \phi_k(\omega_1) \phi'_k(\omega_2). \quad (1.33)$$

Consider now that we have a pair of photons in modes a and b , and another pair of photons in modes c and d , see Figure 1.7(b). These two independent photon sources generate the following states:

$$|\psi_1\rangle_{ab} = \iint d\omega_a d\omega_b f(\omega_a, \omega_b) \hat{a}^\dagger(\omega_a) \hat{b}^\dagger(\omega_b) |0, 0\rangle_{ab} \quad (1.34)$$

$$|\psi_2\rangle_{cd} = \iint d\omega_c d\omega_d h(\omega_c, \omega_d) \hat{c}^\dagger(\omega_c) \hat{d}^\dagger(\omega_d) |0, 0\rangle_{cd}. \quad (1.35)$$

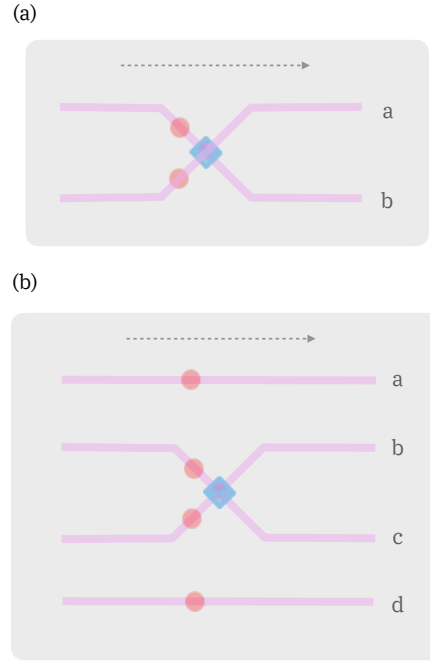


Figure 1.6: Hong-Ou-Mandel interference circuit. Hong-Ou-Mandel interference (HOM) occurs on a beam-splitter (BS) between two modes. The direction of propagation of photons is indicated by the arrow, whilst each of the modes are designated with letters. Interference is shown between two modes in both cases, (a) denotes dependent HOM interference between photons from the same source, whereas (b) shows independent (or heralded) HOM interference between photons from different sources.

The photons in mode c and d possess a joint spectrum defined by $h(\omega_c, \omega_d)$, which is equivalent to Equation (1.33), except the Schmidt coefficients are v_k and the spectral amplitudes are denoted as φ_k and φ'_k . Interference between modes b and c requires us to determine the reduced density operator describing them, which consists of tracing out the discarded modes utilising the partial trace. For an explicit derivation we direct the reader to consult Ref. [59]. The probability of detecting a coincidence between modes b and c is described by,

$$p_{cc}(\tau) = \frac{1}{2} - \frac{1}{2} \sum_{kk'} u_k^2 v_{k'}^2 \int d\omega_b \phi_k^*(\omega_b) \varphi_{k'}(\omega_b) e^{-i\omega_b \tau} \int d\omega_c \varphi_{k'}^*(\omega_c) \phi_k(\omega_c) e^{i\omega_c \tau}. \quad (1.36)$$

Here, one could consider arbitrary spectral function for $\phi(\omega_b)$ and $\varphi(\omega_c)$ to determine what the HOM interference looks like as a function of temporal delay τ .

Referring back to the motivation for deriving what happens when two photons are incident on a BS, we want to be able to characterise, and more specifically benchmark the performance of the source by assessing the implied purity of the photons. Given this, let us focus on how we can determine the visibility and how this helps determine the photon purity.

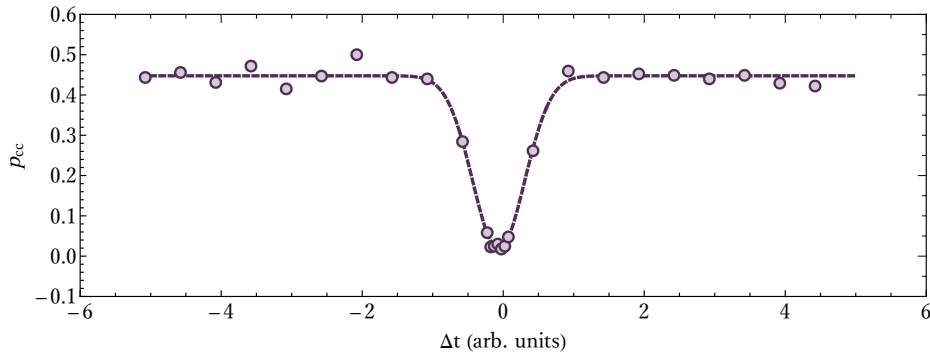


Figure 1.7: Two-photon interference on a beam-splitter. Hong-Ou-Mandel interference as a function of the temporal delay for indistinguishable photons. Upon a beam-splitter, indistinguishable photons undergo bunching at $\Delta t = 0$.

1.5.2.1 Purity and visibility

We will now show how the visibility of the two-photon interference maps to photon purity. The following calculation can also be applied to general two-photon interference, but to act as a suitable benchmark for source quality we need to be able to infer the heralded-photon spectral purity.

Taking up from where we left the independent HOM interference derivation from Equation (1.36), in the two limits of temporal offset $\tau \rightarrow 0$ and $\tau \rightarrow \infty$, and considering the case where we have photons that are both described by the same spectral amplitude i.e. $\phi = \varphi$, Equation (1.36) is simplified to:

$$\begin{aligned} p_{cc}(\tau = 0) &= \frac{1}{2} - \frac{1}{2} \sum_{kk'} u_k u_{k'} \int d\omega_b \phi_k^*(\omega_b) \phi_{k'}(\omega_b) \delta_{kk'} \\ &= \frac{1}{2} - \frac{1}{2} \sum_k u_k^2, \end{aligned} \quad (1.37)$$

for the limit where the temporal offset is 0 and the wave-packets are fully overlapped, whilst for the other extreme:

$$p_{cc}(\tau \rightarrow \infty) = \frac{1}{2} - \frac{1}{2}(0) = \frac{1}{2}. \quad (1.38)$$

Now, we define the visibility of the interaction as

$$\mathcal{V} = \frac{p_{\max} - p_{\min}}{p_{\max}}, \quad (1.39)$$

where $p_{\max} = p_{cc}(\tau \rightarrow \infty)$ and $p_{\min} = p_{cc}(\tau = 0)$. Substituting in our expressions

the visibility now takes the form

$$\mathcal{V} = \frac{\frac{1}{2} - \left(\frac{1}{2} - \frac{1}{2} \sum_k u_k^2\right)}{\frac{1}{2}} = \sum_k u_k^2, \quad (1.40)$$

where remarkably, the visibility of the interaction is equivalent to the purity of the single photon states, $\mathcal{V} = \sum_k u_k^2 = \text{Tr}[\rho_\phi^2] = \mathcal{P}$. Translating this theoretical result into something experimentally measurable, the maximum probability p_{\max} , defines a region where there is a maximum number of coincidence counts. The minimum probability defines a region where there are minimal number of coincidence counts. In turn, these regions physically represent being in the centre of the dip and being sufficiently away from the centre of the dip, or rather in a position that is outside the interference region. Figure (??) shows the probability of detecting a coincidence as a function of the temporal delay, exhibiting the so-called HOM dip between independent sources. The experimental measure for the visibility requires the number of detected photon coincidence counts in the centre of the dip N_{cc}^{in} and the number of detected photon coincidence counts in a position sufficiently away from the dip N_{cc}^{out} , and is thus defined as:

$$\mathcal{V} = \frac{N_{cc}^{\text{out}} - N_{cc}^{\text{in}}}{N_{cc}^{\text{out}}} = 1 - \frac{N_{cc}^{\text{in}}}{N_{cc}^{\text{out}}}. \quad (1.41)$$

Crucially, a point of insight on heralded-photon interference that will be revisited when discussing an experiment investigating the performance of photon sources, is that the above calculations hold under the assumption that one and only one photon exists in each input on the BS. Realistically however, one should consider that the photon number statistics of the photon source may cause more than one photon in each mode at a time, degrading the measured visibility and thus purity.

Chapter 2

A Source of Photons

2.1	Parametric Down Conversion	24
2.1.1	Generating PDC photons	24
2.1.1.1	Departing from a Classical Approach	28
2.2	Down-converted Photon Spectra	31
2.2.1	Pump Envelope Function	32
2.2.2	Phase-matching Function	33
2.2.3	Joint Spectral Amplitude	36
2.2.3.1	Factorisation of the Joint Spectra	37
2.3	Photon Number Statistics	39
2.3.1	Modelling Photon Rates	39
2.3.2	Heralding and Brightness	42
2.4	Concluding remarks	43

Over the past century, experimental investigations into everything from settling foundational arguments within quantum mechanics to performing interesting quantum information processing protocols have used non-linear effects to generate single photons. The interplay of three optical fields, or three-wave mixing, nominally describes the range of effects that are subsequent from media exhibiting non-linear effects to to the second order (the third order is four-wave mixing, not a focus of this thesis but may be mentioned in passing). These effects are far from new and have therefore been investigated, developed and refined for many different applications within science.

2.1 Parametric Down Conversion

Parametric down-conversion (PDC) is one of the processes that has benefitted from these investigations and developments and is therefore one of the most widely used mechanisms for generating photons. Whilst different media are capable of supporting PDC, the focus of this thesis is on potassium titanyl phosphate (KTP). The description of PDC within this work is not confined to this material, but it is a non-centrosymmetric material (a requirement for materials to exhibit strong enough non-linearities) which forms the basis of discussion within subsequent chapters. It is an understatement to say that there are many sources of material which discuss and detail the process of PDC, many in much greater detail than what follows. However, as the basis of this thesis follows a story-line that relies on understanding PDC to begin with, sufficient details will be given on how one theoretically derives important features of the PDC process such as the pump envelope function and the phase-matching function.

2.1.1 Generating PDC photons

Non-linear optics describes the interaction of light with matter, specifically in the case where the response of the material is not linear when a large electric field is applied to it. Linear optical processes are described by:

$$\hat{P}(t) = \varepsilon_0 \chi^{(1)} \hat{E}(t), \quad (2.1)$$

where the polarisation response of the material $\hat{P}(t)$, is proportional to the electric field $\hat{E}(t)$ that is applied to the material (via the linear susceptibility $\chi^{(1)}$ and the permittivity ε_0). In the presence of a strong electric field, the simple linear relation no longer holds true as a good approximation. We must however, consider non-linear terms and expand Equation (2.1) to include appropriate dependencies on higher order terms,

$$\begin{aligned}\hat{P}(t) &= \varepsilon_0 \left[\chi^{(1)} \hat{E}(t) + \chi^{(2)} \hat{E}^2(t) + \chi^{(3)} \hat{E}^3(t) + \dots \right] \\ &= \hat{P}^1(t) + \hat{P}^2(t) + \hat{P}^3(t) + \dots\end{aligned}\tag{2.2}$$

where $\chi^{(2)}$ and $\chi^{(3)}$ are the second and third order optical susceptibilities of the material respectively [60]. The susceptibility term $\chi^{(n)}$, decreases rapidly for magnitudes of $n > 1$. For most media $n = 1$, hence why only certain media can exhibit non-linear optical effects. Of particular interest are the second order terms, which only emanate in non-centrosymmetric materials. This is because $\chi^{(2)}$ is actually a tensor $\chi_{i,j,k}^{(2)}$, where i, j, k are cartesian coordinates. A crystal is said to be non-centrosymmetric when the material is not invariant upon rotations around the z axis. Invariance upon rotation means that the optical response of the medium will be the same for an electric field polarised in the x or the y direction, such that $\chi_{z,x,x}^{(2)} \equiv \chi_{z,y,y}^{(2)}$, and under these conditions non-linear susceptibilities vanish. For more in depth details on the role of symmetry in non-linear optics (and also how group theory is used to classify classes of crystals), consult Ref. [61]. A specific non-linear interaction involving the second order non-linear susceptibility $\chi^{(2)}$ known as *down-conversion* is of particular interest for optical quantum information processing, as it can be used to produce photon pairs. The $\chi^{(2)}$ interaction consists of an input *pump* photon “converting” into a *signal* photon and *idler* photon under energy conservation laws.

Let us derive some important components behind down-conversion. To understand this “conversion”, we need to consider an incident field $\hat{E}(t)$, which is a superposition of two monochromatic waves with frequencies ω_1 and ω_2 , interacting in a medium capable of supporting non-linear optical effects. Substituting the incident field

$$\hat{E}(t) = E_1 e^{-i\omega_1 t} + E_2 e^{-i\omega_2 t} + c.c.,\tag{2.3}$$

into Equation (2.2) and isolating only the second order terms, yields a non-linear

polarisation response according to,

$$\begin{aligned} \hat{P}^2(t) = \varepsilon_0 \chi^{(2)} & \left[E_1^2 e^{-2i\omega_1 t} + E_2^2 e^{-2i\omega_2 t} + \right. \\ & \left. 2E_1 E_2 e^{-i(\omega_1 + \omega_2)t} + 2E_1 E_2^* e^{-i(\omega_1 - \omega_2)t} + c.c. \right] + \\ & 2\varepsilon_0 \chi^{(2)} \left[E_1 E_1^* + E_2 E_2^* \right]. \end{aligned} \quad (2.4)$$

The amplitude of each component of Equation (2.4) can be expressed as a function of different frequencies ω_j . Each of these components describes various $\chi^{(2)}$ optical processes:

$$P(2\omega_1) = \varepsilon_0 \chi^{(2)} E_1^2 e^{-2i\omega_1 t} \quad (2.5)$$

$$P(2\omega_2) = \varepsilon_0 \chi^{(2)} E_2^2 e^{-2i\omega_2 t} \quad (2.6)$$

$$P(\omega_1 + \omega_2) = 2\varepsilon_0 \chi^{(2)} E_1 E_2 e^{-i(\omega_1 + \omega_2)t} \quad (2.7)$$

$$P(\omega_1 - \omega_2) = 2\varepsilon_0 \chi^{(2)} E_1 E_2^* e^{-i(\omega_1 - \omega_2)t} \quad (2.8)$$

$$P(0) = 2\varepsilon_0 \chi^{(2)} (E_1 E_1^* + E_2 E_2^*). \quad (2.9)$$

These equations express a variety of non-linear optical processes. Equation (2.5) and (2.6) both describe *second-harmonic generation*, Equation (2.7) describes *sum-frequency generation*, Equation (2.8) *difference-frequency generation* and finally Equation (2.9) describes *optical rectification*. Of particular interest is sum-frequency generation (SFG), where oscillations of generated fields are twice that of the incident fields. PDC is effectively the reverse process of SFG, where a strong pump field is (partially) converted into two fields of lower energy (conserving energy). The properties of PDC means the process is incredibly well suited for pseudo on demand, but probabilistic photon generation.

Using a semi-classical approach, we can model the propagation of a field through a non-linear medium to investigate this process some more. A monochromatic plane wave propagating through a non-linear medium can be modelled using Maxwell's equations:

$$\nabla^2 \hat{E} - \frac{1}{c^2} \frac{\partial^2}{\partial t^2} (\hat{E} + \frac{\hat{P}}{\varepsilon_0}) = 0. \quad (2.10)$$

By expanding the brackets, this equation can be rearranged to take the form,

$$-\nabla^2 \hat{E} + \frac{1}{c^2} \frac{\partial^2}{\partial t^2} \hat{E} = -\frac{1}{\varepsilon_0 c^2} \frac{\partial^2}{\partial t^2} \hat{P}. \quad (2.11)$$

We ultimately want to arrive at an equation which relates the non-linear polarisation response of a medium, to an applied electric field. We consider two well spaced frequency waves, and a nonlinear polarisation response for each incident field:

$$\hat{E}_1 = E_1 e^{i(k_1 z - \omega_1 t)}, \quad (2.12)$$

$$\hat{E}_2 = E_2 e^{i(k_2 z - \omega_2 t)}, \quad (2.13)$$

$$\hat{P}_1^{NL} = P_1^{NL} e^{i(k_1 z - \omega_1 t)}, \quad (2.14)$$

$$\hat{P}_2^{NL} = P_2^{NL} e^{i(k_2 z - \omega_2 t)}. \quad (2.15)$$

The polarisation response of the medium is defined as,

$$\hat{P} = \hat{P}^{(1)} + \hat{P}^{NL} \quad (2.16)$$

where $\hat{P}^{(1)}$ is the linear polarisation response of the media and \hat{P}^{NL} is the non-linear response. Substituting Equation (2.1) into the above equation we obtain an expression for the polarisation response that we can substitute into Equation (2.11). Using $n^2 = 1 + \chi^{(1)}$, expanding and rearranging we have,

$$-\nabla^2 \hat{E} + \frac{n^2}{c^2} \frac{\partial^2}{\partial t^2} \hat{E} = -\frac{1}{\epsilon_0 c^2} \frac{\partial^2}{\partial t^2} \hat{P}^{NL}. \quad (2.17)$$

Knowing that the wave-vector is defined,

$$k_i^2 = n_i^2 \frac{\omega_i^2}{c^2},$$

making the appropriate substitutions and only considering propagation along the z direction, we can finally arrive at,

$$\frac{dE_i(z, t)}{dz} e^{ik_i z} = \frac{i\omega_i}{2\epsilon_0 n_i c} P_{\omega_i}^{NL}(z). \quad (2.18)$$

From here, all one needs to do to obtain the resulting amplitudes $E(z)$, of different waves propagating through a non-linear medium, is express $P_{\omega_i}^{NL}(z)$ in terms of input field amplitudes $E_i(z)$. But in order to be capable of fully describing PDC, we must leave a semi-classical treatment of non-linear optical effects. We want to

concern ourselves with the case where an intense pump field ω_3 , is converted into an ensemble of two conjugate fields ω_1 and ω_2 , such that $\omega_3 = \omega_1 + \omega_2$. If we consider our pump field to be a photon, and our signal and idler (output) fields to also be photons, then we have the case described by $\hbar\omega_3 \longrightarrow \hbar\omega_1 + \hbar\omega_2$ —a process where one photon “disappears” to generate two photons under conservation of energy. This process is fully described by an effective Hamiltonian meaning that we must leave a semi-classical approach and adopt a fully quantum mathematical treatment.

2.1.1.1 Departing from a Classical Approach

To derive a quantum Hamiltonian, we need an expression for the energy of the system. This is given by [62],

$$H(t) = \int d^3r \left[\int_0^{\hat{H}(t)} \hat{B}(t) \cdot \delta\hat{H}'(t) + \int_0^{\hat{D}(t)} \hat{E}(t) \cdot \delta\hat{D}'(t) \right], \quad (2.19)$$

where $\hat{H}(t) = \hat{B}(t)/\mu_0$ for materials that do not exhibit any magnetic properties. The polarisation response of a material $\hat{P}(t)$, is related to the displacement field $\hat{D}(t)$ by

$$D_i(t) = \varepsilon_0 E_i(t) + P_i(t). \quad (2.20)$$

If we express Equation (2.19) (after substituting Equation (2.2) and Equation (2.20)), whilst only considering terms that depend on $\chi^{(2)}$, we get the Hamiltonian that describes the mixing of three fields:

$$H_I(t) = \varepsilon_0 \int d^3r \chi_{ijk}^{(2)} E_i(t) E_j(t) E_k(t). \quad (2.21)$$

This is where all the interaction dynamics are contained. Using to the Schrödinger equation the interaction will evolve according to,

$$\hbar \frac{\partial}{\partial t} |\psi(t)\rangle = \hat{H}_I(t) |\psi(t)\rangle, \quad (2.22)$$

and has the solution:

$$|\psi\rangle_{\text{out}} \approx \exp\left[\frac{-i}{\hbar} \int_{-\infty}^{\infty} dt \hat{H}_I(t)\right] |\psi\rangle_{\text{in}}. \quad (2.23)$$

The approximation arises from the non-commutative nature of the interaction Hamiltonian with itself at different times. A time ordering operator is required, in order to express the above equation explicitly, but the non-trivial effects introduced by the operator are only present in a high-gain regime [63–65]. Given that we will only be considering low pump powers we assume that we can neglect the effects that occur in the using the high gain regime. We must also make some further assumptions and assume that the propagation of all fields are collinear along the z axis, and that propagation occurs throughout a non-linear medium that has a length L . We further assume that this medium only supports one transverse mode (restriction in the $x - y$ planes), therefore reducing this scheme to one dimension. The quantisation of the electromagnetic field via a plane wave expansion means we can express the electric field operator as [62],

$$\hat{E}_{i,\omega_0}(\vec{r}, t) = i \int d\omega \sqrt{\frac{\hbar\omega_0}{4\pi c\epsilon_0 n(\omega_0)}} \left[\xi_i(x, y) \hat{a}_i(\omega) e^{i(kz - \omega t)} - \xi_i^*(x, y) \hat{a}_i^\dagger(\omega) e^{-i(kz - \omega t)} \right]. \quad (2.24)$$

Here, the only transverse mode supported by our non-linear medium is described by $\xi(x, y)$ and is appropriately normalised. We know that in the case being considered, we have three fields. Each one of these fields have non-overlapping frequencies with central frequencies ω_1 , ω_2 and ω_3 , together with orthogonal components of polarisation. Each orthogonal component of the polarisation is a sum of all three of the fields (ω_1 , ω_2 and ω_3) for that polarisation state, with the index i denoting the direction of polarisation,

$$\hat{E}_i(\vec{r}, t) = \hat{E}_{i,\omega_1}(\vec{r}, t) + \hat{E}_{i,\omega_2}(\vec{r}, t) + \hat{E}_{i,\omega_3}(\vec{r}, t). \quad (2.25)$$

Introducing the above equation into the interaction Hamiltonian we obtain an abundance of terms. Most of these terms we will be neglected and our discussion will only continue with terms that contain three different fields i.e $\hat{E}_{\omega_1} \hat{E}_{\omega_2} \hat{E}_{\omega_3}$. Interestingly, from some of these terms we can observe other non-linear optical effects such as type-I PDC, where both output fields have the same polarisation and orthogonal

polarisations to the pump field. The interaction Hamiltonian then becomes,

$$\begin{aligned}
\frac{-i}{\hbar} \int_{-\infty}^{\infty} dt \hat{H}_I(t) &= \frac{\chi^{(2)}}{2} \sqrt{\frac{\hbar \omega_{01} \omega_{02} \omega_{03}}{\varepsilon_0 \pi^3 n_1 n_2 n_3}} \int dt dz d\omega_1 d\omega_2 d\omega_3 [\\
&N_1 e^{i(k_1+k_2+k_3)z - i(\omega_1+\omega_2+\omega_3)t} \hat{a}_1 \hat{a}_2 \hat{a}_3 + \\
&N_2 e^{i(k_1+k_2-k_3)z - i(\omega_1+\omega_2-\omega_3)t} \hat{a}_1 \hat{a}_2 \hat{a}_3^\dagger + \\
&N_3 e^{i(k_1-k_2+k_3)z - i(\omega_1-\omega_2+\omega_3)t} \hat{a}_1 \hat{a}_2^\dagger \hat{a}_3 + \\
&N e^{i(k_1-k_2-k_3)z - i(\omega_1-\omega_2-\omega_3)t} \hat{a}_1 \hat{a}_2^\dagger \hat{a}_3^\dagger - h.c.].
\end{aligned} \tag{2.26}$$

where in the final line we have $N = \int dx dy \xi_1(x, y) \xi_2^*(x, y) \xi_3^*(x, y)$, which is the overlap of the transverse field modes. Only the variables that are conjugated alter in the different terms $N_i \in \{N_1, N_2, N_3, N\}$ that appear in each line of Equation (2.26). The final four lines also differ in terms of the creation and annihilation operators, for example, $\hat{a}_1 \hat{a}_2 \hat{a}_3^\dagger$ represents the annihilation photons at frequencies ω_1 and ω_2 and the creation of a photon at frequency ω_3 . Likewise, we can see that $\hat{a}_1 \hat{a}_2^\dagger \hat{a}_3^\dagger$ creates two photons at frequencies ω_2 and ω_3 whilst a photon at frequency ω_1 is annihilated, the essence of PDC. One could compute the z dependent integrals in Equation (2.26), using

$$\int_{-a}^a dx e^{ixy} = \frac{2}{y} \sin(ay) = 2a \operatorname{sinc}(ay),$$

where knowing that the t dependent integrals result in delta functions with factors 2π allows us to cancel out dependencies on ω_1 . We will only include the computed t dependent integrals, and leave the z dependent integral unchanged for reasons that will be discussed in Section 2.2.2. Equation (2.26) can be reduced further by neglecting terms which do not satisfy conservation of energy and momentum condition, $\omega_1 = \omega_2 + \omega_3$, which in terms of wave-vectors reads $k_1 - (k_2 + k_3) \approx 0$. This leads to the condition, $\Delta k \approx 0$. As the interaction occurs over the length of the crystal L the output state that contains $\hat{a}_1 \hat{a}_2^\dagger \hat{a}_3^\dagger$ is derived by inserting the Hamiltonian into Equation (2.23). We obtain:

$$|\psi\rangle_{\text{out}} = \exp\left(2\pi\Theta \iint d\omega_2 d\omega_3 \int dz g(z) e^{i\Delta k(\omega_2, \omega_3)z} \alpha(\omega_2 + \omega_3) \hat{a}_2^\dagger(\omega_2) \hat{a}_3^\dagger(\omega_3) - h.c.\right) |\psi\rangle_{\text{in}}. \tag{2.27}$$

All the constants, as well as the overlap of the transverse field modes are gathered into,

$$\Theta = \frac{\chi^{(2)}}{2} \sqrt{\frac{\hbar\omega_{01}\omega_{02}\omega_{03}}{\varepsilon_0\pi^3n_1n_2n_3}} N. \quad (2.28)$$

We denote $\phi(\Delta k(\omega_2, \omega_3)) = \int dz g(z) e^{i\Delta k(\omega_2, \omega_3)z}$ thus forth, where $g(z)$ is the non-linearity profile along the crystal. As previously mentioned, the inclusion of this un-computed integral will be explained in Section 2.2.1. We also express

$$A(\omega_2 + \omega_3) = \hat{a}_1(\omega_2 + \omega_3).$$

The left hand side of which is equates to, $\sqrt{I/\hbar\omega_1}\alpha(\omega_2 + \omega_3)$, where I is the pulse energy of the pump and $\alpha(\omega_2 + \omega_3)$ is a normalised frequency distribution that satisfies $\int d\omega_1 |\alpha(\omega_1)|^2 = 1$ and $\alpha(\omega_1) = \alpha(\omega_2 + \omega_3)$. Finally then, after a Magnus expansion (explicitly shown in Ref. [63]), we can write the output PDC state as:

$$\boxed{|\psi\rangle_{\text{out}} = \iint d\omega_2 d\omega_3 \phi(\Delta k(\omega_2, \omega_3)) \alpha(\omega_2 + \omega_3) \hat{a}_2^\dagger(\omega_2) \hat{a}_3^\dagger(\omega_3) |0\rangle.} \quad (2.29)$$

This is a crucial equation in the context of this thesis. It is the explicit output state of the PDC process. We can envelop the functions $\phi(\omega_2, \omega_3)$ and $\alpha(\omega_2 + \omega_3)$ that are contained within the above equation, into a single function. This is commonly known as the joint spectral amplitude (JSA) and contains all the spectral properties of the PDC process. More explicitly, it is the product of the *phase-matching function* (PMF) and the *pump envelope function* (PEF),

$$f(\omega_2, \omega_3) = \phi(\omega_2, \omega_3) \alpha(\omega_2 + \omega_3). \quad (2.30)$$

For the subsequent section, and also the majority of this thesis, I shall refer to the output photons with frequencies ω_2 and ω_3 , as *signal* and *idler* photons respectively, whilst the input photon with frequency ω_1 will be referred to as the *pump*.

2.2 Down-converted Photon Spectra

The JSA plays an important role within the PDC process and also the subsequent sections and chapters of this thesis. PDC creates a two-photon state, the spectral properties of which are fully described by the JSA. As stated in the previous section,

the JSA is a product of the PMF and the PEF. The PEF represents the characteristics of the pump photon. The PMF represents the material properties, and as you will be shown later in Section 2.2.2, relies on a-priori knowledge of the frequency-dependent refractive index. To determine the frequency dependent refractive index we rely on the Sellmeier equations [66], which are typically written as,

$$n^2(\lambda) = 1 + \sum_j \frac{A_j \lambda^2}{\lambda^2 - B_j}. \quad (2.31)$$

Here, λ is the wavelength and A_j and B_j are determined empirically and depend on the material in question. There are correction factors and temperature dependencies that one could also add to obtain the refractive index change over a wide range of wavelengths (with a higher degree of precision). These will not be mentioned any further but can be found for most materials. The material we focus on in this thesis is KTP, and coefficients and correction factors for the Sellmeier equations can be found within Refs. [67, 68]. In this work we will be working with specific wavelengths. The pump photon is centred at 775nm which under the degeneracy condition, down-converts to photons centred at 1550nm.

2.2.1 Pump Envelope Function

The PEF characterises the spectral properties of the pump photon. Conservation of energy dictates the relation between the pump photon and the signal and idler photons which is also reflected in the PEF, where $\alpha(\omega_p) = \alpha(\omega_s + \omega_i)$. The joint distribution therefore, lies along a diagonal line spanning from top-left to bottom-right and satisfies the energy conservation condition. The resulting PEF is depicted in Figure (2.1).

Typically, within this thesis, the PEF will be treated as a squared *hyperbolic secant* (sech) function, as it is the typical temporal shape of a short pulse from a mode-locked laser. The only other PEF mentioned in this thesis will be a Gaussian. Whilst the Gaussian pulses are transform limited, the $\text{sech}^2(t/\tau)$ pulses may not be, and thus suffer from chirping. A full analysis of the effects of a chirped non-transform limited pulse on the PDC bi-photon spectra can be found in Ref. [69].

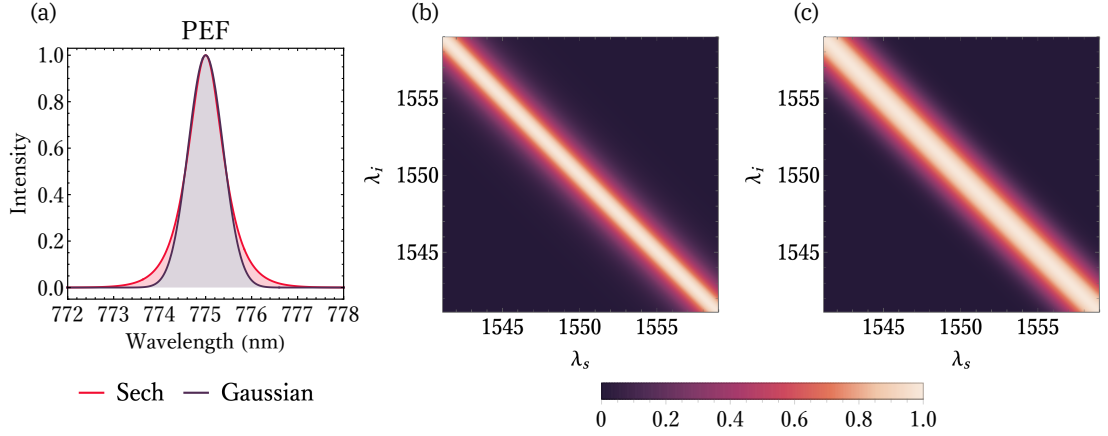


Figure 2.1: Visualising the pump envelope function corresponding to a sech profile or Gaussian profile, in terms of both the temporal intensity (a), and spectral profiles, (b) and (c). The spectral profiles are theoretical PEFs based on a temporal pulse duration of 1.4ps. From inspection, the sech spectral profile (b) is narrower than the Gaussian spectral profile (c), a feature of the sech and Gaussian temporal profiles as a relationship of the pump pulse duration. The temporal profiles in (a) are sech and Gaussian functions plotted with different pump pulse durations to match FWHMs.

Here, we do not consider the affects of chirping and define the PEF as,

$$\alpha_{\text{PEF}}(\omega_s, \omega_i) = \text{sech}\left[\left(\omega_s + \omega_i\right)\frac{\pi\tau}{2}\right], \quad (2.32)$$

where τ is a temporal scaling factor. Figure (2.1) depicts details about the PEF.

A variable of importance in the context of the PEF, is the pump pulse duration. Longer pump pulses result in narrower PEF width and vice-versa. When one seeks high purity photons—under the assumption that the PEF and PMF assume Gaussian functions or near Gaussian functions—the width of the PEF should match the width of the PMF [69].

2.2.2 Phase-matching Function

Unlike how the PEF aligns itself along the diagonal, the PMF can be vastly different. As mentioned earlier, we consider the down-converted photon wavelengths centred at 1550nm. Depending on desired wavelengths, the analysis of PDC no longer becomes universal and can be very different. The phase-matching condition for generating down-converted photons with KTP at 1550nm is approximately linear but, as an example, for highly non-degenerate PDC that produces down-converted photons at say 800nm and 1550nm, the phase-matching is not a straight line in the joint

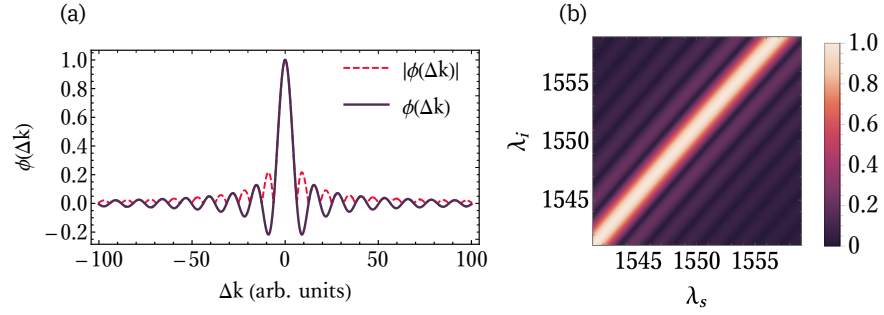


Figure 2.2: Phase-matching function. For a bulk crystal, the effective non-linearity is a step function which, in the Fourier domain, is a sinc function. In Δk space (a), the side lobes are observable. In terms of the bi-photon state, the PMF as a function of the down-converted photon wavelengths (b), the sinc intensity is still observed. Details of this figure will be discussed later on.

frequency space¹, see Figure (2.3). But before going into the details as to why, we need to look at the PMF in finer detail.

Generally the PMF is given by:

$$\phi(\Delta k(\omega_s, \omega_i)) = \int_{-\infty}^{\infty} g(z) e^{i\Delta k(\omega_s, \omega_i) z} dz, \quad (2.33)$$

where $\Delta k(\omega_s, \omega_i)$ is the phase mismatch and $g(z) = \chi^{(2)}(z)/\chi_0^{(2)}$ is the normalised non-linearity along the crystal profile. Of particular importance to us is the fact that $g(z) = 1$ along the length of the crystal and $g(z) = 0$ outside the crystal boundaries. Take note of this point as it will be discussed later when we introduce more succinct details regarding photon source designing. Equation (2.33) is an improper integral, and when evaluated over the length of a crystal L becomes,

$$\phi(\Delta k(\omega_s, \omega_i)) = \int_0^L g(z) e^{i\Delta k(\omega_s, \omega_i) z} dz = L e^{i\Delta k(\omega_s, \omega_i) L/2} \text{sinc}\left[\Delta k(\omega_s, \omega_i) \frac{L}{2}\right]. \quad (2.34)$$

This is representative of the PMF of a bulk crystal. The nonlinearity in this case, is effectively a step function, defined by the boundaries of the crystal. Just like how computing the integral in Equation (2.34) produces a *sinc*, the Fourier transform of a step function, also produces a *sinc* function. Whilst not of significant importance just now, this function will be discussed in the following chapter, so the readers attention may be drawn back to Figure (2.2) to observe the prevalent side lobes that are associated with the sinc function.

Going back to the discussion on Equation (2.34), for maximum amplitude, the

¹There are also cases, where the phase-matching curve is so far from non-linear, that two down-conversion processes occur simultaneously [70].

condition $\Delta k(\omega_s, \omega_i) = 0$ is required. Explicitly this term is the phase (or momentum) mismatch which is written as,

$$\Delta k(\omega_s, \omega_i) = k(\omega_s + \omega_i) - k_s(\omega_s) - k_i(\omega_i), \quad (2.35)$$

and is governed by the aforementioned Sellmeier equations. It is possible for this condition not to be satisfied and in most general cases it is not. This will be discussed in more detail later on when the quasi-phase-matching technique is introduced, but for now our discussion focuses on the phase-mismatch explicitly. Depending on the wavelengths being analysed, the true relation between the wavelength and momentum mismatch requires the expansion of the wave number to the first order, $k_j(\omega) = k_j(\omega_{0_j}) + \Omega_j v_j^{-1}$, where v_j is the group velocity $v_j = d\omega/dk_j(\omega_{0_j})$. The term ω_{0_j} is a central reference frequency and has been introduced to account for any shifts away from this wavelength. To account for these shifts we have introduced $\Omega_j = \omega_j - \omega_{0_j}$. As a function of the signal and idler wavelengths, the momentum mismatch is important to consider. To the first order, the momentum mismatch becomes:

$$\Delta k(\omega_s, \omega_i) = \Delta k_0 + (v_p^{-1} - v_s^{-1})\Omega_s + (v_p^{-1} - v_i^{-1})\Omega_i, \quad (2.36)$$

where $\Delta k_0 = k_p(\omega_{0_s} + \omega_{0_i}) - k_s(\omega_{0_s}) - k_i(\omega_{0_i})$. When considering a small spectral ranges the momentum mismatch seems to obey an approximately linear relation. Plotting the above equation as a function of the frequency shifts around the desired down-converted photon wavelengths defines an angle θ that is related to the group velocities of the pump, signal and idler photons via,

$$\tan(\theta) = -\frac{v_p^{-1} - v_s^{-1}}{v_p^{-1} - v_i^{-1}}. \quad (2.37)$$

A desired angle can be obtained through careful considerations of the group-velocities. This technique is referred to as group-velocity matching (GVM) and is a lossless way to remove spectral correlations [71–73]. For our application, we would like this angle to be close to 45° —as shown in Figure 2.3—to meet the so called symmetric GVM condition. The symmetric GVM condition is a special case where $v_p^{-1} = (v_s^{-1} + v_i^{-1})/2$. To generate the full PMF, the final step is to explicitly calculate the non-linear response of the crystal as a function of Δk , and map that response onto the momentum mismatch as a function of the signal and idler frequencies. We

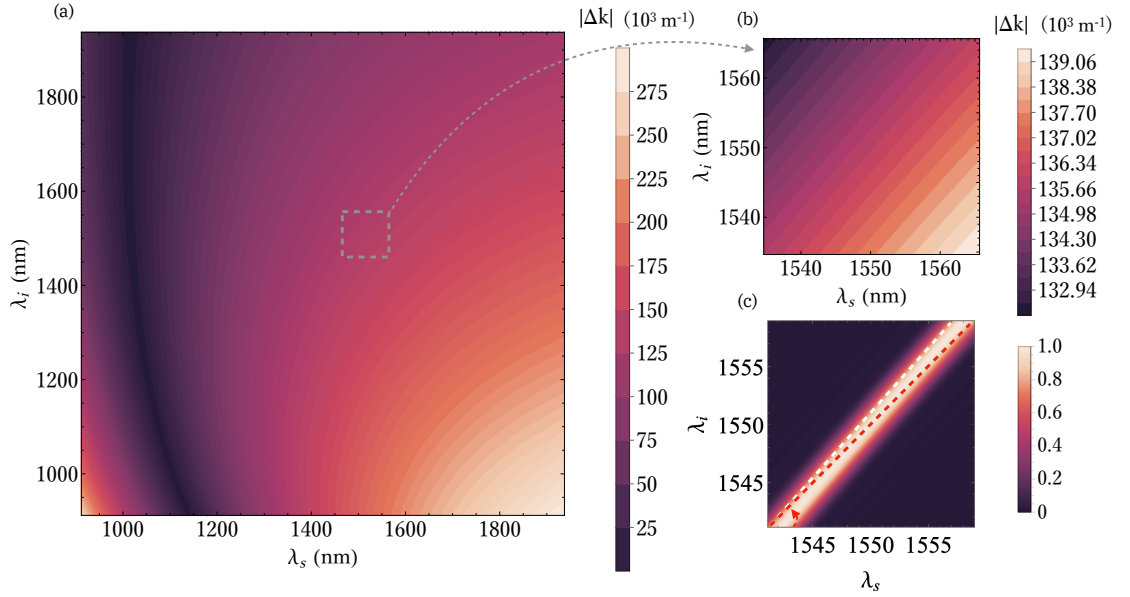


Figure 2.3: Phase mismatch and PMF spectrum. These figures highlight some important features of the momentum mismatch in KTP, specifically plotting Equation (2.2.2) in figures (a) and (b) with large and small spectral ranges respectively. When small ranges are considered, a linear relation between momentum mismatch and wavelengths works as a good approximation. Highlighted in (c), selecting appropriate group-velocities defines an angle across the joint spectra (red dashed line representing 45°).

direct the reader’s attention back to Figure (2.2)(b), where the above remarks are captured concluding with the PMF.

2.2.3 Joint Spectral Amplitude

Now we have obtained the PMF and the PEF, the final step to obtain the JSA is to simply multiply these two functions together; the product and components of this multiplication are shown in Figure 2.4. The JSA contains all the spectral information of the PDC state. Within this thesis, an alternative description of the joint photon spectra is frequently used. Due to the nature of experimental reconstructions, measurements of the joint spectral intensity (JSI) are much more common than measurements of the JSA. Explicitly, the JSI is just the absolute value of the JSA squared,

$$\text{JSI} = |\text{JSA}|^2.$$

We will reveal some subtleties about the outcome of using the JSI instead of the JSA to draw conclusions about spectral correlations and the photon purity in Chapter 3.

Within Chapter 3, we also direct discussions towards obtaining spectrally pure photons. An important metric, of particular concern within this thesis, is the de-

degree of separability of the bi-photon PDC state which governs the purity of down-converted photons. In the following section we will highlight the interplay of separability and purity.

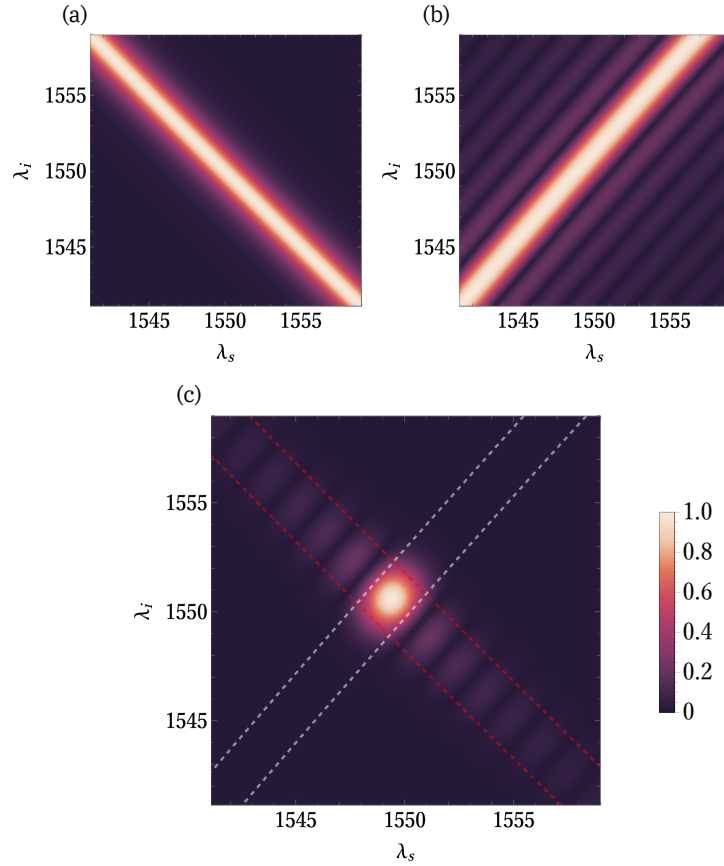


Figure 2.4: Joint spectral amplitude and its components. The joint spectral amplitude (c) is composed of the PEF (a) and PMF (b). The contours highlighted on the JSA are for the PEF (red) and the PMF (white). Whilst not of great importance now, the spectral correlations are easily seen in this figure. The side lobes from the PMF (b) are very much present in the JSA (c). When measuring one of the two photons the JSA describes, the photon that is not measured, is projected into a statistical mixture of orthogonal spectral states.

2.2.3.1 Factorisation of the Joint Spectra

An important property of a photon is its spectral purity. Much more detail about photon purity will be discussed later on, however understanding how one quantifies how pure a photon is—from its spectral properties—will be discussed in this section. Typically the aim of the work contained in this thesis, is high purity photons. This means the outcome of most mathematical journeys will be 1, representing unit photon purity. A note for the reader; obtaining unit purity is not the goal for all experiments invoking PDC, epitomised by the work presented within Appendix B. For unit photon purity, correlations in the spectral degree of freedom need to be

removed. The JSA can reveal the purity of the bi-photon state by means of *Schmidt decomposition* (SD) [74].

In order to understand how the separability criteria effects the photon purity, we need to express the down-converted state as a product of orthogonal basis vectors. This can be done using the SD, expressing the bi-partite system as a set of unique and complete set of basis vectors. We can write the decomposed, two-photon state as,

$$|\psi\rangle_{\text{pair}} = \sum_k b_k |q_k\rangle_s |r_k\rangle_i, \quad (2.38)$$

with Schmidt coefficients b_k that satisfies normalisation criteria, and Schmidt modes defined as: $|q_k\rangle_s = \int d\omega q_k(\omega) |\omega\rangle_s$ and $|r_k\rangle_i = \int d\omega r_k(\omega) |\omega\rangle_i$. This helps us reveals some information about what happens when we herald the presence of one of the daughter photons. The heralding can be understood as a projector defined as,

$$\hat{C}_i = \int d\omega |\omega\rangle_i \langle\omega|_i = \sum_k |r_k\rangle\langle r_k|. \quad (2.39)$$

The heralded state can be calculated by applying the Born rule and tracing out the detected photon leading to,

$$\rho_s = \text{Tr}_i[|\psi\rangle_{\text{pair}} \langle\psi|_{\text{pair}} (\mathbf{1} \otimes \hat{C}_i)] \quad (2.40)$$

$$= \sum_k b_k^2 |q_k\rangle\langle q_k|. \quad (2.41)$$

In the case where one of the daughter photons is detected, let's say the signal photon, then the idler photon mode is traced over. This leaves the state of the heralded photon in a statistical mixture of single photon states with orthogonal spectral distributions. This statistical mixture is exactly what leads to spectral correlations and photon distinguishability. The heralded photons purity is given by,

$$\text{Tr}[\rho_s^2] = \sum_k b_k^4.$$

The purity can range from $\mathcal{P}_s = 1$ for a completely pure state (our goal), to $\mathcal{P}_s = 1/N$ —where N is the number of Schmidt modes—for a completely mixed state with. The requirement therefore for a pure state is therefore the existence of only one Schmidt mode.

2.3 Photon Number Statistics

Ultimately, PDC is not limited to the production of just a single pair of photons. Knowledge of the PDC state beyond the first order is crucial. Understanding how photon number statistics behave as a function of not only pump power, but also as a function of the number of pair sources, is crucial for multi-photon experiments. This is so that one could estimate the rate at which multi-photon events can occur and understand how the signal-to-noise ratio (SNR) may scale. The photon number pair production and multi-pair production can be calculated knowing the statistical behaviour of the photon source and sets of functions for determining how measured photon rates can translate to photon rates before detection.

Within the context of photon source designing, the brightness of a source is some what entwined with the photon number purity, and an understanding of the metrics used in the following sections of this chapter will be useful for the rest of this thesis. To motivate the need of understanding photon source statistics, consider the scenario that you are planning an eight-photon experiment and you want to understand the parameter space you have access to, namely the brightness, pump power, repetition rates and detection efficiency. This understanding is important when there are realistic limits to consider such as the amount of accessible pump power, detection reset times and the fact one wants to operate in with a sufficient signal-to-noise ratio. If one has explicit knowledge, or at least a good estimate of the photon source behaviour for a variety of the parameters accessible to the experimenter, then they can make a decision with regards to optical arrangement for said source i.e. the required pump power, repetition rate and focussing conditions.

2.3.1 Modelling Photon Rates

In order to gain knowledge of the squeezing parameter γ —which governs the probability of pair generation—we need the single rates and the raw coincidence rate as a function of the pump power. The probability that the non-linear photon source produces n photons is given by,

$$(1 - P_{\tau})(P_{\tau})^n = (1 - \gamma^2)(\gamma^2)^n, \quad (2.42)$$

where τ is a constant that determines the interaction strength within the media given a pump power of P [75, 76]. The probability can also be expressed with respect to the squeezing parameter which is related to pump power via $\gamma = \sqrt{P\tau}$. The γ parameters importance is evident when you express the down-conversion process as a series expansion of photon number terms in signal and idler modes:

$$\begin{aligned} |\psi\rangle_{\text{PDC}} &= \sqrt{1 - \gamma^2} \sum_{n=0}^{\infty} \gamma^n |n, n\rangle \\ &= \sqrt{1 - \gamma^2} (|0, 0\rangle + \gamma |1, 1\rangle + \gamma^2 |2, 2\rangle + \dots). \end{aligned}$$

The parameter γ now dictates the probability of photon pair emission. For example the probability of generating n -pairs of photons being generated is $\sqrt{1 - \gamma^2} \gamma^n$ where we observe the characteristic polynomial scaling of PDC sources. If we want to obtain a four-fold coincidence events then typically we seek the $n = 1$ generation in two separate crystals with the same pump pulse. However, due to probabilistic nature of these photon sources, having two independent sources producing $n = 1$ pairs of photons is probabilistically equivalent to having a single source producing $n = 2$ pairs. This a particularly important issue to consider when planning multi-photon experiments.

To model the photon generation we begin with a geometric distribution which governs photon number statistics from pulsed sources. The probability of n -fold emission is,

$$p_{\text{em}}(P, n, \tau) = (1 - P\tau)(P\tau)^n. \quad (2.43)$$

We deploy superconducting nanowire single photon-detectors (SNSPDs) to detect the arrival of a photon. These are non-number resolving detectors which simply click when $n > 0$ photons arrive. If we consider n photons generated, we may only be capable of detecting k out of n photons due to the operational nature of the SNSPDs. The detection probability of detecting at least k photons given n photons in a single mode is therefore given by [51],

$$p_{\text{det}}(\eta, n, k) = 1 - \sum_{m=0}^{k-1} \binom{n}{m} \eta^m (1 - \eta)^{n-m}, \quad (2.44)$$

where η is not just the detection efficiency of the detector present in the mode, but also the transmission probability associated to that mode. An additional function

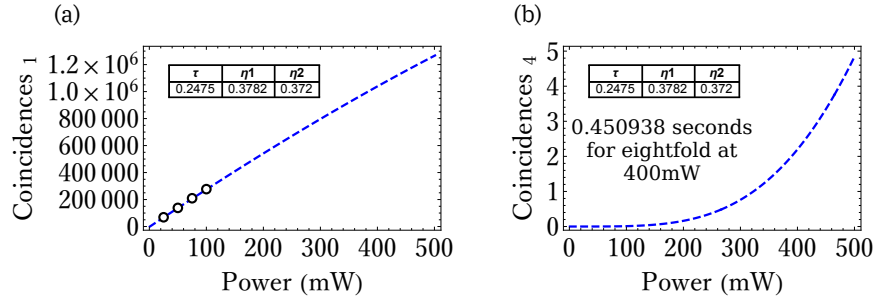


Figure 2.5: Using a suitable model for the generation rates from our photon source in order to predict multi-photon rates. An example of how we model photon rates to help us map detection of two-folds (a) to prospective eight-fold generation rates (b). These plots were generated during our attempts to determine what repetition rate we would need in order to obtain sufficient eight-fold coincidences.

which adds extra accuracy in representing the final photon number statistics of our system is the probability that the detectors, which have an associated dead-time after a detection event, are ready to detect photons again. The probability that a detector is ready is the probability that firstly, photons are emitted from the source combined secondly, with the probability that within a time window t —equivalent to the dead-time associated with that detector—no photon was detected. This is written as,

$$p_{\text{ready}}(P, R, t, \tau, \eta_1, \eta_2) = \left[\sum_{i=0}^{\infty} p_{\text{em}}(P, i, \tau) \cdot p_{\text{det}}(1 - \eta_1, i, i) \cdot p_{\text{det}}(1 - \eta_2, i, i) \right]^{\lfloor R \times t \rfloor}, \quad (2.45)$$

where R is the repetition rate of our pump in Hz, t is the detectors dead-time, and the exponent is wrapped in a floor function which rounds to the nearest integer that is less or equivalent to the value the function is being applied to. With these three functions we can now begin to build a model which approximates the photon rates we expect to see post detection. For the rates of single photon detection the function reads as,

$$R_s(P, R, t, \tau, \eta) = R \left(\left[\sum_{j=1}^{\infty} p_{\text{em}}(P, j, \tau) \cdot p_{\text{det}}(\eta, j, 1) \right] p_{\text{ready}}(P, R, t, \tau, \eta, 0) \right) \quad (2.46)$$

For multi-photon experiments we are interested in rates of coincidences from N -

photon sources, the probability of such events are,

$$R_{cc}(P, R, t, \tau, \eta_{m_1}, \eta_{m_2}, N) = R \cdot \prod_{m=1}^N \left(p_{\text{em}}(P, j, \tau_m) \cdot p_{\text{det}}(\eta_{m_1}, 1, 1) \cdot p_{\text{det}}(\eta_{m_2}, 1, 1) \cdot p_{\text{ready}}(P, R, t, \tau_m, \eta_{m_1}, \eta_{m_2}) \right), \quad (2.47)$$

where we have assigned distinct spatial modes m_1 and m_2 . Using these functions we can approximately extract the parameters τ , η_1 and η_2 for each source from empirical data sets. This is achieved by minimising the following:

$$\begin{aligned} & |s_1(P) - R_s(P, t, \tau, \eta_1)| + |s_2(P) - R_s(P, t, \tau, \eta_2)| \\ & + |cc(P) - R_{cc}(P, t, \tau, \eta_1, \eta_2)|, \end{aligned} \quad (2.48)$$

given that we know measured single and coincidence rates, s_1, s_2 and $cc_{1,2}$, as a function of the pump power. We can measure the repetition rate, the detector dead-times and thus obtain numerical values for τ , η_1 and η_2 . These values can then be re-used inside Equation (2.47) to output the expected rates from N sources just with data corresponding to the performance of a single source. For example Figure (2.5) takes the measured two-fold rates and applies the model to extract τ , η_1 and η_2 to let us estimate the expected eight-fold rates if we so desire.

2.3.2 Heralding and Brightness

An important metric, mentioned already, but mainly throughout the subsequent parts of this thesis, is the symmetric heralding efficiency. Consider a pair of daughter photons generated when a PDC source is triggered, producing a bi-photon state. The heralding efficiency is the probability of detecting a daughter photon, conditioned on having already detected the other daughter photon constituting the pair.

Let us now explicitly go through how the heralding efficiency is defined as it sometimes varies slightly in literature. We measure the *symmetric* heralding adhering to the following mathematical definition which will be using throughout the rest of this thesis. To arrive at this condition consider that the amount of loss incurred by each mode of the PDC state, is η_k . Then, the generation rate (given a source brightness β) of singles in mode k is,

$$s_k = \beta \eta_k.$$

The probability of generating a single in both signal and idler modes, equivalent to a coincidence (cc), is therefore,

$$p(s_s, s_i) = \beta \eta_s \eta_i \equiv cc_{s,i}. \quad (2.49)$$

Gathering individual efficiencies of each mode into one term, $\eta = \sqrt{\eta_s \eta_i}$, the final expression for heralding efficiency requires one to rearrange Equation (2.49) for η_s and η_i , to get to,

$$\eta = \frac{cc_{s,i}}{\sqrt{s_s s_i}}. \quad (2.50)$$

2.4 Concluding remarks

Within this chapter we introduced most of the preliminary and broader aspects surrounding PDC photon sources, specifically with KTP. We also narrowed our analysis to the case where we have a pump photon with a central wavelength of 775nm producing degenerate photons with central wavelengths of 1550nm. The following chapter takes the concepts from this chapter such as the PMF and the JSA, and goes into more detail on how one can use techniques to alter the PMF and as a consequence the JSA, producing photons with desired characteristics.

Chapter 3

Photon source for multi-photon state generation

3.1	Optimised photon source	45
3.1.1	Source design	46
3.1.2	Domain engineering	48
3.1.2.1	Obtaining a Gaussian PMF	49
3.1.3	Tracking algorithm for domain engineering	52
3.1.4	Focusing conditions	54
3.2	Experimental analysis of source performance	55
3.2.1	Source preparation	56
3.2.2	Independent Hong-Ou-Mandel	58
3.2.3	Reconstructing the Joint Spectrum	62
3.2.3.1	Elongation of Joint Spectrum	65
3.3	Concluding remarks	65
3.3.1	Acknowledgements	66

So far our discussion about PDC has been somewhat broad, but in this section, we will focus on how one can obtain pure, separable photons in the telecom-C band. A few prerequisites for the reader: we desire both daughter photons to be the same wavelength (degenerate condition), to be in the telecom-C band, to be spectrally pure, and to be generated at sufficient rates.

Obtaining high spectral purity directly from the PDC process, removes the need to employ spectral filters. If we cast the readers attention back to the note we made in the previous section about the side-lobes generated by the step in non-linearity (Figure (2.2)), we can see that tight spectral filters with bandwidths comparable to the width of central peak, will help filter out spectral side-bands and increase the spectral purity of down-converted photons. There are several caveats to this technique, such as reductions to photon number purity and reduced heralding efficiencies, but these will be discussed in more detail in following sections of this chapter. So that we can remove the filtering requirement, the PMF must be altered. Photon source engineering can achieve this task and in this Chapter we discuss the culmination of experimental work in photon source engineering, obtaining a source operating on the achievable limit of bulk PDC. Possessing a source of pure photons, capable of high rates and with high heralding efficiencies enables scalability, crucial when we move to multi-qubit experiments in the latter parts of this thesis.

3.1 Optimised photon source

In order to build multi-qubit states efficiently, we require efficiently generated photons with high indistinguishability for two key conditions. Firstly, two-photon interference is a fundamental part in the building of multi-qubit states, and to minimise errors in this interaction the only option is to use indistinguishable photons. Secondly, in order to overcome unfavourable loss scalings, a high heralding efficiency is an absolute necessity. Domain engineering techniques with PDC sources negates the need for lossy spectral filtering allowing one to satisfy these conditions inherently within the source design.

3.1.1 Source design

In order to get into the grittier details of source designing, we need to visit the broader topics we discussed in the previous chapter. One aspect of photon source designing we discussed was GVM. What we concluded from that discussion was, generating photons at desired wavelengths, requires the phase-matching condition to be satisfied, conserving momentum in the PDC process. In most cases, computing Equation (2.36) for desired wavelengths results in $\Delta k(\omega_s, \omega_i) \neq 0$, rendering this process seemingly unachievable. There is however, a technique to ensure that at your desired wavelengths, the phase-matching condition and momentum conservation is satisfied. *Quasi-phase-matching* (QPM) was first introduced in Ref. [77, 78], and is discussed in detail within Ref. [79]. Rather than using isotropic material for the PDC process, the premise of QPM is to periodically alter the structure of the material. These periodic alterations are, explicitly, the act of inverting the ferroelectric domains of the material every coherence length. The coherence length ℓ_c , is the length at which the relative phase of the two down-converted fields changes by π . As a result of QPM an additional term is introduced into Equation (2.36) such that the equation becomes,

$$\Delta k(\omega_s, \omega_i) = k(\omega_s + \omega_i) - k_s(\omega_s) - k_i(\omega_i) + \frac{2\pi}{\Lambda} \quad (3.1)$$

where $\Lambda = 2\ell_c$ shifts the peak of the PMF to satisfy momentum conservation and produce photons at desired wavelengths. To be more accurate however, one needs to follow closely both Refs. [79, 80], which include how this additional term affects the shape of the PMF in Δk space, something that most textbook discussion on QPM omit. Incorporating the new phase-mismatch from periodic poling the explicit PMF—Equation 3.1—becomes,

$$\phi(\Delta k(\omega_s, \omega_i)) = \frac{2}{\pi} \cdot z e^{i\Delta k(\omega_s, \omega_i)z/2} \operatorname{sinc}\left[\frac{\Delta k(\omega_s, \omega_i)z}{2}\right]. \quad (3.2)$$

The reader was told to take note of the role of $g(z)$ within Equation (2.2.2), the above equation is a direct result of a combination of $g(z)$ now retaining the values of $+1$ or -1 due to the periodic flips to the domains, the additive property of the PMF and the effects of the additional term $2\pi/\Lambda$.

So far we have discussed what QPM is, but have only briefly mentioned the

effects of implementing QPM. The best way to understand the effects of introducing periodic poling is to compare the PMF at $\Delta k = 0$, and shifts away from this condition, along the z axis of a crystal, this is shown in Figure 3.1(a) and (b) respectively. Firstly, this figure highlights the fact that the amplitude of phase-matched bulk KTP is greater than that of periodically-poled KTP (ppKTP), an important feature to note when we start considering domain engineering. A reduced amplitude of the PMF in this picture, represents a reduction in effective non-linearity strength, a reduced τ in Equation (2.42), and therefore results in a lower probability of pair production.

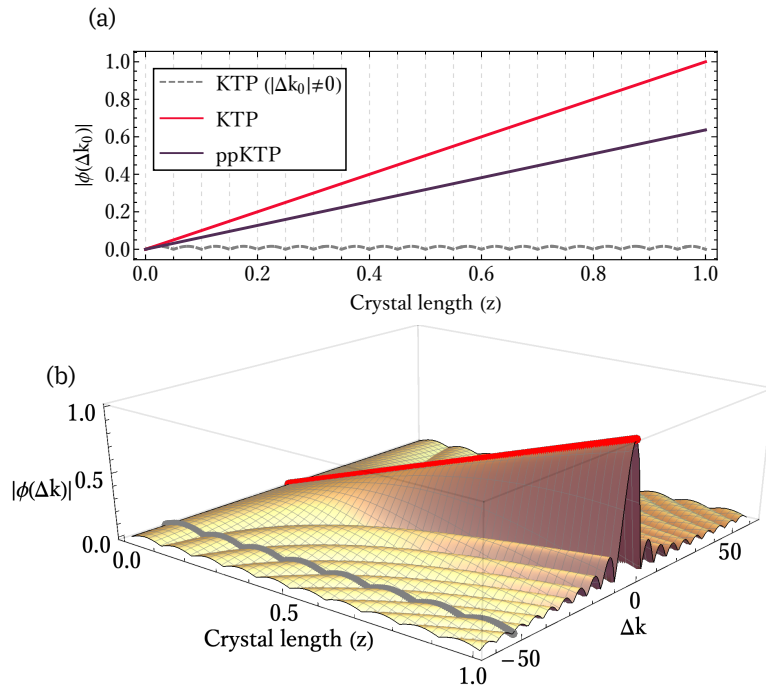


Figure 3.1: PMF of a bulk crystal and a comparison of a bulk crystal with a periodically poled crystal. Comparing the amplitude of the PMF (a) for bulk KTP (labelled as just KTP in the plot), whilst (red) and whilst not (grey dashed) meeting the momentum conservation criteria. When the momentum conservation is not conserved then the PDC process is not supported and the amplitude of the PMF fails to grow shown by the grey dashed line. When the momentum conservation is satisfied, the gradient of the PMF for bulk KTP is maximal. Introducing periodic poling, can ensure that the field does grow along the length of the crystal, but the gradient of this growth is restrained for reasons shown in deriving Equation 3.2. We can also show the effects of deviations away from ideal momentum conservation with a 3D plot shown in (b), as well as the purity degrading side lobes resulting from the interaction.

Now that we have discussed QPM, which introduces the notion of altering the domain structure of a crystal, we can introduce the idea of using this concept to not only satisfy the momentum-conservation but to also reshape the PMF in order to produce spectrally pure photon pairs. To realise this idea, we officially begin our

journey into domain engineering, and the techniques wherein altering the spectra of the bi-photon state is achieved via specific crystal design considerations.

3.1.2 Domain engineering

Altering the structure of the domains is not limited to the case of simple periodic inversions. On numerous occasions now we have mentioned the fact that, ideally, the generated photons should be spectrally pure. Unfortunately, up to now, the PDC sources we have discussed thus far, all suffer from the same detrimental spectral correlations. These arise from the inextricable link between the shape of the nonlinearity profile and the PMF, via the Fourier transform. As long as there is a step in the nonlinearity profile of the crystal, the PMF will contain spectral correlations. The easiest way to understand this is to consider the case for bulk KTP and ppKTP, where the nonlinearity profile is a step function. Inside the boundaries of the crystal, the nonlinearity is uniform, outside the boundaries the effective nonlinearity is zero creating a step—and thus producing fluctuations in the Fourier space—leading to side-lobes adjacent to the peak of the PMF. This is present in Figure 2.2(a)¹. The main purpose of employing domain engineering therefore, is to alter the nonlinearity profile, removing any “steps” in nonlinearity, culminating in producing a PMF free of side-lobes adjacent to the main peak.

Domain engineering, before its proposal to help in removing spectral correlations from bi-photon states, was a well studied concept in nonlinear optics, shaping and compressing pulses in second harmonic generation [81–83].

Extending these techniques to PDC means it is in-fact entirely possible to remove all spectral correlations via domain engineering. A neat and well known property of Gaussian functions, is that their Fourier transform, is a Gaussian. The relation between nonlinearity and PMF therefore means a Gaussian nonlinearity profile will produce a Gaussian PMF. The first attempt to realise a Gaussian PMF was performed by Brańczyk *et al.* in Ref. [84]. Approximating a Gaussian PMF with step functions of different heights—a result of different orders of periodic poling along the length of the crystal—the authors verified that they obtained a Gaussian PMF via two-photon interference in the manner we discussed in Section 1.5.2.1. Since

¹Still a rather hand-wavy discussion however, more discussion centred around this insight will be had later in this chapter; where also, a more detailed figure will aid the reader into visualising this effect.

then, techniques for obtaining a Gaussian PMF have become more refined, and deviate slightly away from this initial concept. Briefly, these techniques come under the descriptions of altering the poling duty cycle of the crystal domains [85–88], the orientation of the poling direction [89], and tailoring both [90–92]—all generating the desired Gaussian function to an approximation.

Moving away from a general description of domain engineering techniques, the following work in this chapter is focused on using optimal techniques for Gaussian PMF shaping outlined and developed in Ref. [92].

Graffitti *et al.* then used one of the techniques to demonstrate, for the first time, interference of photons generated from independent domain-engineered crystals in Ref. [90]; A crucial step for photon sources whose purpose is to create multi-qubit quantum states.

3.1.2.1 Obtaining a Gaussian PMF

For now, we will outline how we design a crystal to generate pure photons. The method used in this work follows a technique outlined in Ref. [92] (discussed in more detail later) which in turn closely relates to the technique outlined in Ref. [91], except the technique is modified by means of tailoring a crystal with a pre-defined and fixed domain widths. Subsequently in Ref. [92], a more advanced technique was also introduced that can shift the boundaries of the domains via a pre-existing annealing algorithm, which was initially developed for semi-classical optimisation of higher harmonic processes [81, 93]. This advanced technique is not required for Gaussian PMF shaping but the technique, developed primarily for generating separable photons, can also be exploited for tailoring high quality non-Gaussian PMFs, e.g. for efficient generation of time-frequency mode entanglement [94], contained in Appendix B, and time-frequency hyper-entanglement [95].

To begin the design process, the initial step in the process is to define a target PMF function, which for reasons already outlined, will be a Gaussian with some width σ and centred at Δk_0 ,

$$\phi_{\text{target}}(\Delta k) = e^{-\frac{1}{2}(\Delta k - \Delta k_0)^2 \sigma^2}. \quad (3.3)$$

Computing the Fourier transform of this function provides us with the nonlinearity

profile:

$$\begin{aligned} g_{\text{target}}(z) &= \mathcal{F}[\phi_{\text{target}}(\Delta k)] = \int_{-\infty}^{\infty} \frac{1}{\sqrt{2}} \phi_{\text{target}}(\Delta k) e^{i\Delta k z} d\Delta k \\ &= \frac{1}{\sigma} e^{-\frac{z^2}{2\sigma^2} + i\Delta k_0 z}. \end{aligned} \quad (3.4)$$

Obtaining the PMF along the length of the crystal requires an inverse Fourier transform. The subtlety here, rather than just going back and forth between Equation (3.3) and Equation (3.4), is to incorporate the finite and fixed length of the crystal along the z axis. We therefore need to consider that a crystal lies in the region defined by $z \in [-l/2, l/2]$. The inverse Fourier transform then, is performed between the limits defined by the crystals region, in turn giving us the Fourier transform of the PMF along the whole length of the crystal, depicted in Figure (3.2). Computing this gives us the mathematical form of the function used in order to obtain the correct domain structure of the crystal via a tracking technique,

$$\begin{aligned} \phi_{\text{track}}(\Delta k; z) &= \int_{-\frac{l}{2}}^z g_{\text{target}}(z') e^{-i\Delta k z'} dz' \\ &= \sqrt{\frac{\pi}{2}} e^{-\frac{\sigma^2(\Delta k - \Delta k_0)^2}{2}} \left[\text{erf} \left(\frac{l - 2i\sigma^2(\Delta k - \Delta k_0)}{2\sqrt{2}\sigma} \right) \right. \\ &\quad \left. + \text{erf} \left(\frac{z + i\sigma^2(\Delta k - \Delta k_0)}{\sqrt{2}\sigma} \right) \right]. \end{aligned} \quad (3.5)$$

Interestingly this function reveals a critical element concerning the crystals design which is important not to overlook. For regions outside the boundaries of the crystal $\phi_{\text{track}}(\Delta k; z) \neq 0$. This is the result for a function that mathematically may not, and does not, equate to 0 outside these boundaries. Unless special considerations are made with respect to the target function width σ , the Gaussian function defined in Equation 3.3, may yet still contribute purity degrading side-lobes. We will specifically discuss this point once we address the final issue with the function we arrived at in Equation (3.5). In order to obtain the final mathematical form of our function, we need to apply a scaling factor. We mentioned already in Section 3.1.1, that transitioning from bulk KTP to ppKTP via QPM, meant the amplitude of the PMF was reduced, shown in Figure 3.1. The maximum gradient of a poled crystal is $2/\pi$ and mapping this maximum gradient onto the function we arrived at for tracking, means that we ensure the amplitude of the PMF is maximal and photon generation is maximised for the conditions we have chosen. This is done by finding

the maximum gradient of the function we currently have for tracking,

$$\frac{d}{dz} \phi_{\text{track}}(\Delta k; z) = -\frac{\left(z - \frac{l}{2}\right) e^{-\frac{\left(z - \frac{l}{2}\right)^2}{2\sigma^2}}}{\sigma^3}, \quad (3.6)$$

$$\max\left[\frac{d}{dz}\phi_{\text{track}}(\Delta k; z)\right] = \frac{1}{\sigma}, \quad (3.7)$$

and defining a variable ζ that is scaled to the maximum gradient $2/\pi$:

$$\zeta = \frac{2}{\pi} \frac{1}{\max\left[\frac{d}{dz}\phi_{\text{track}}(\Delta k; z)\right]} = \frac{2\sigma}{\pi}. \quad (3.8)$$

This variable can now be multiplied to our tracking function. Finally then, we simplify our function somewhat by fixing the phase matching condition, $\Delta k = \Delta k_0$, and shifting the position of the crystal to occupy a region defined by $z \in [0, l]$ by shifting $z \rightarrow z - l/2$ giving:

$$\zeta \sqrt{\frac{\pi}{2}} \left(\operatorname{erf}\left(\frac{l}{2\sqrt{2}\sigma}\right) + \operatorname{erf}\left(\frac{z - \frac{l}{2}}{\sqrt{2}\sigma}\right) \right) \quad (3.9)$$

Now, we can move onto a required discussion we hinted towards earlier on in our outline of the domain engineering process: the width of the target Gaussian function σ . This parameter ultimately balances source brightness with spectral purity. Broadly speaking, in order to obtain high source brightness the function must be wide, but to avoid unwanted spectral correlations, the function must be narrow. Thus we choose a width that both avoids a large step in non-linearity—avoiding

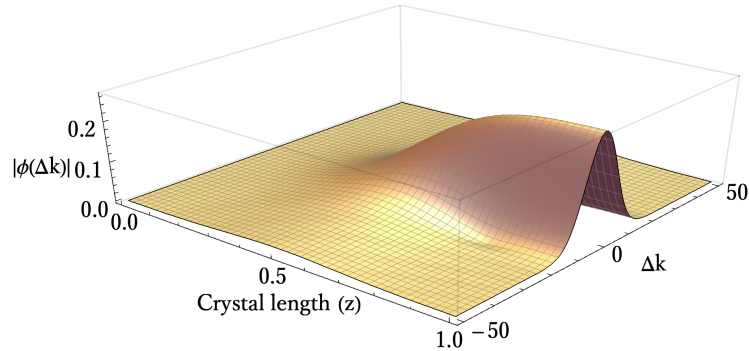


Figure 3.2: Full PMF from target function. The PMF $\phi_{\text{track}}(\Delta k; z)$ with Δk centred at 0, along the full length of the crystal as defined by Equation (3.5). The important feature of this figure is the shape of the PMF once the function has been integrated over the whole length of the crystal. Comparing this Figure to Figure (3.1)(b), it is clear that the shape of the PMF, at the full length of the crystal ($z = 1$), does not contain any side-lobes.

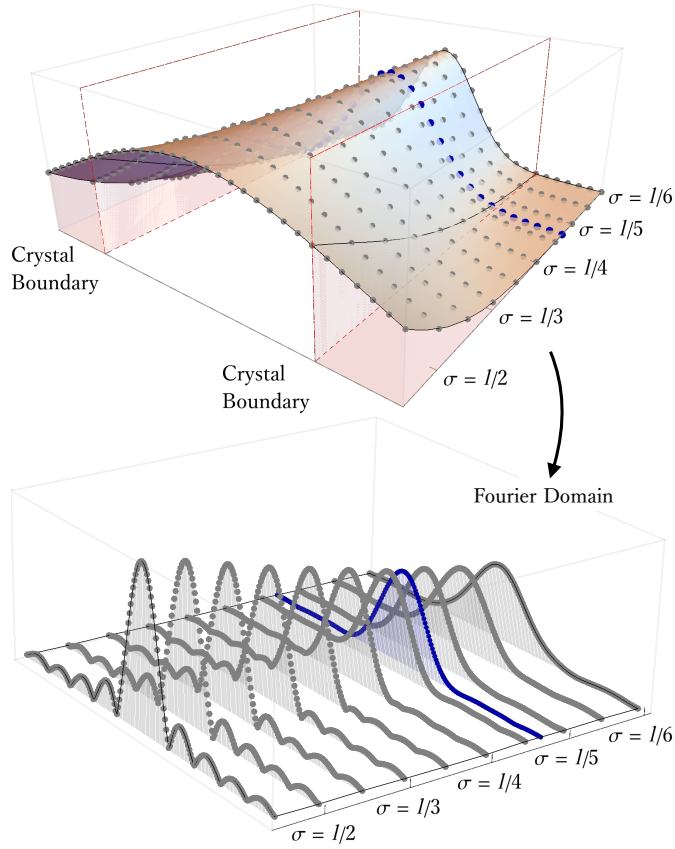


Figure 3.3: Target function for Gaussian domain engineering. The top panel shows the target function of varying widths, with the red shaded areas indicating regions outside the boundary fixed by the crystal length l . A target function that is too wide, for example when $\sigma = l/2$, will result in side lobes in the PMF which is shown on the bottom panel. A narrow target function may produce minimal side lobes in the PMF, but will result in a lower effective non-linearity and therefore a lower source brightness. The blue dotted lines indicate the trade-off we chose for our implementation.

spectral correlations—whilst wide enough to obtain a reasonably high effective non-linearity and thus brightness. This trade-off is illustrated in Figure 3.3. With a $\sigma = l/4.7$, where l is the crystal length, the generation of side lobes is minimal whilst not adversely reducing generation rates. For a crystal length of $l = 30$ mm, $\sigma = 6.38$ mm. There is no analytical solution for the ideal width, however there is a deeper discussion with more empirical evidence as to why a $\sigma \sim l/5$ is a good choice, within Ref [80].

3.1.3 Tracking algorithm for domain engineering

Only when a suitable PMF is defined can we consider how we go from having the explicit mathematical form the function to be tracked, ϕ_{track} , to getting a KTP crystal with exactly the properties we would expect. To obtain a crystal with a

domain structure that defines a desired PMF, we need a suitable algorithm that tracks ϕ_{track} , and by this we mean that each ferroelectric domain in the crystal is orientated a way to reproduce ϕ_{track} . There are a variety of techniques for tracking a function. Initially pioneered by Ref. [91], more tracking algorithms have been proposed and a nice overview of these techniques can be found in Ref. [80].

Each ferroelectric domain can be orientated either “Up” or “Down”. The aim of the algorithms is to determine whether a domain should be orientated “Up” or “Down” by evaluating a cost function. Each algorithm differs slightly in its technique and also its ability. For the purpose of obtaining a crystal with a Gaussian PMF the “one-domain block” algorithm is most suitable. Starting with a seed domain structure, where each domain is fixed to a width equal to the coherence length ℓ_c the algorithm assess whether it is converging towards its target, ϕ_{track} , via an error function,

$$e(z + \ell_c) = \phi_{\text{track}}(\Delta k_0; z + \ell_c) - \phi_{\text{eff}}(\Delta k_0; z). \quad (3.10)$$

This evaluates the difference between the generated PMF ϕ_{eff} and the desired PMF ϕ_{track} for each domain. Starting at the first domain and iterating along the crystal, the algorithm handles the task of determining whether to orientate the next domain in the “Up” orientation, or the “Down”. Explicitly the algorithm follows the following arguments:

- if $e(z + \ell_c) \geq 0$ and $\phi_{\text{track}}(\Delta k_0; z) \geq \phi_{\text{track}}(\Delta k_0; z - \ell_c)$, flip the domain orientation with respect to the previous domain, meaning ϕ_{eff} continues to increase.
- if $e(z + \ell_c) \geq 0$ and $\phi_{\text{track}}(\Delta k_0; z) \leq \phi_{\text{track}}(\Delta k_0; z - \ell_c)$, keep the domain orientation consistent with the previous domain, causing ϕ_{eff} to begin increasing.
- if $e(z + \ell_c) < 0$ and $\phi_{\text{track}}(\Delta k_0; z) \geq \phi_{\text{track}}(\Delta k_0; z - \ell_c)$, keep the domain orientation consistent with the previous domain, causing ϕ_{eff} to begin decreasing.
- if $e(z + \ell_c) < 0$ and $\phi_{\text{track}}(\Delta k_0; z) \leq \phi_{\text{track}}(\Delta k_0; z - \ell_c)$, flip the domain orientation with respect to the previous domain, meaning ϕ_{eff} continues to decrease.

This algorithm is more flexible and more accurate than the “two-domain block” algorithm, meaning that for a fixed crystal length and specific target functions, it

can better replicate the desired PMF. A finer discretisation of the domain structure could also be incorporated into tracking algorithms [92], that is domain widths smaller than the coherence length ℓ_c . This is a particularly useful technique for short length crystals phase-matched for shorter temporal pulses and tracking functions that contain more features, such as the target PMF in Appendix B.

3.1.4 Focusing conditions

The final subsection before we discuss the experimental results from our customised aperiodically-poled KTP (aKTP), is dedicated to the optical conditions in which the PDC crystal is placed. Brightness and heralding efficiencies are crucial parameters for photon sources, and are intrinsically linked to the focussing parameters. Furthermore, down-converted photons are not typically left to propagate through free space, but are coupled into single-mode fibres. As a result, there have been numerous theoretical and experimental investigations into the best focusing conditions for maximal heralding efficiencies and source brightness, and the best practices for the efficient collection of signal and idler photons.

An in-depth study made by Bennink in Ref. [96], which has been verified experimentally [97–100], showed that for pump, signal and idler photons that exist in a Gaussian spatial mode and propagate co-linearly, a dimensionless focusing parameter can be defined:

$$\xi_k = \frac{l}{k_k \omega_k^2} = \frac{l}{2z_{Rk}}. \quad (3.11)$$

This parameter—for a crystal length l , defined for mode k —helps quantify the capable brightness and heralding efficiency of the PDC source, and the trade-offs there after. The main insight from this model, and useful conclusions we use in the remaining parts of this thesis, is that a strong pump focussing condition ($\xi \gg 1$) the photon pair coincident rate is high. Opposed to this condition, when the pump focus condition is loosened ($\xi \ll 1$) heralding efficiencies can in principle reach unity, at the expense of the pair generation rate. This has been experimentally verified and also something we investigated with our aKTP crystals. Unfortunately, there is no single set of ξ_k parameters that are universally “optimal”, rather there is a series of curves defined for each parameter that is changed, including the focusing conditions for the collection optics. Decisions on all focusing conditions therefore, should be

made on a case-by-case basis².

It is important not to forget that if raw generation rate is what one seeks, then applying tight focusing and increasing brightness also increases the probability of emission of $n > 1$, i.e higher order pair emission. If the proposed experiment in which you require high rates is sensitive to photon number and higher order generation then consider how you wish to extinguish the generated noise.

From my experiences working with these PDC sources, I would suggest finding a suitable focussing regime to work in by evaluating the needs of the experiment along with the amount of pump power³ available. A decision should then be made in conjunction with the model presented in Section 2.3.1. Within the limit of achievable pump power, do you obtain sufficient rates derived from calculating the effective squeezing γ required from the experiment and provided from your laser? If so, then maximise your heralding by loosening the focusing conditions ensuring that the minimum squeezing and thus count rate you require can still be obtained.

Finally, the reason we also highlight focusing conditions is that a comparison of PDC sources becomes very tricky. Typically, the source brightness and photon indistinguishability is nominally quoted with respect to the amount of power pumping the crystal. In the following experimental section, we address the fact that appropriate source performance levels should be quoted at levels of effective squeezing γ instead. This way, sources which operate with difference focusing conditions can still be compared and contrasted by comparing at the same effective squeezing.

3.2 Experimental analysis of source performance

In Section 1.5, we introduced the concept of two-photon interference. We concluded that, in the case of mixed, identical and completely separable photons, the visibility of the HOM dip is a means of establishing a lower bound on the photon purity. Given the experimental accessibility of two-photon interference measurements, as opposed to phase reconstructed JSA measurements, the HOM visibility is our main metric for how our aKTP crystals perform. This is also pertinent given that PDC source scalability relies on probabilistic fusion gates, the operating principles of which rely on high photon indistinguishability (and thus high purity).

²The most significant finding from Ref. [96], was that for $\xi_p, \xi_s, \xi_i \sim 2, 5$, the brightness, heralding and spectral purity were substantial fractions of their maxima.

³Average power, not peak power. All references to power will be referencing average power.

In this section we will present a culmination of efforts to design the ideal PDC crystal for our use case, and for the parameters in our experimental lab. The following is based on Ref. [101], presenting a telecom-wavelength parametric down-conversion photon source that operates on the achievable limit of domain engineering.

Establishing a benchmark for our newly designed crystal; we use the experimental work in Ref. [90], where a symmetric heralding efficiency of 65% was achieved along with a source brightness of 4kHz/mW and lower-bound photon purity of $90.7 \pm 0.3\%$. Through fine tuning parameters such as the maximal gradient we were capable of generating photons from independent sources achieving two-photon interference visibilities of up to $98.6 \pm 1.1\%$ under similar experimental conditions as the benchmark work (in terms of filtering and optical arrangement). As a consequence of designing a more optimal PMF, we reached net heralding efficiencies of up to 67.5%, which corresponds to collection efficiencies exceeding 90%. We also form a comprehensive comparison between our aKTP crystals, and a very common alternative source constituting ppKTP crystals with filters possessing a very narrow bandwidth (which were both manufactured by Raicol Crystals Ltd.). The reason this comparison is drawn is that typical multi-photon experiments that do not employ any sort of PMF engineering require tight spectral filtering to obtain sufficient two-photon visibilities. This ensures that the spectral purity is high, but is met with the unavoidable consequence of adversely effects attainable heralding efficiencies [38, 102], something highlighted in the following experimental analysis.

3.2.1 Source preparation

Using a mode-locked Ti:Sapphire laser with a non-ideal sech^2 -shaped spectral envelope we pump our crystals at a wavelength of 774.9 nm, down-converting to 1549.8 nm. Obtaining down-converted photons at just below 1550nm was necessary to ensure temperature stabilisation and maintenance of the degeneracy condition, enabled by keeping our crystals sufficiently far from room temperature. The pulse duration of this laser can be tuned to operate at pulse durations around 1.3 ps and 1.4 ps in order to match pulse durations to different crystal and filter combinations. Optical components within the laser cavity introduce positive group velocity dispersion and therefore pulse broadening. To alter the output pulse duration of the

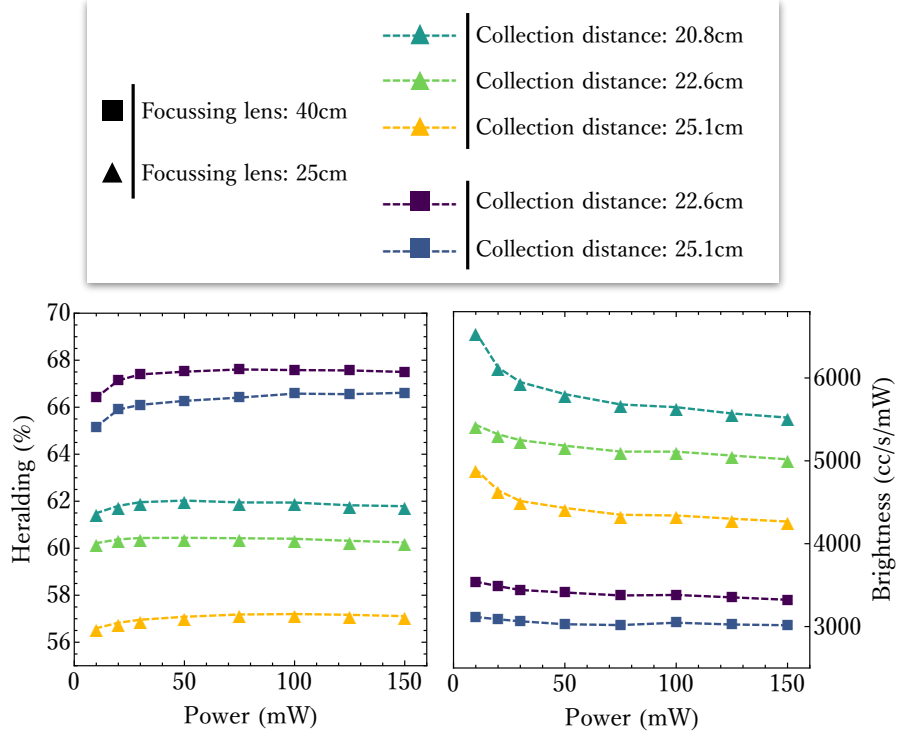


Figure 3.4: Brightness and heralding efficiencies with respect to different pump focusing conditions. Experimentally observed heralding and brightness values for different combinations focussing lens and collection distances. In order to find good experimental condition where we want to validate the performance of our aKTP crystal we ran a series of quick tests to quantify the performance of the crystal. A longer focal length lens creates a larger beam waist and a longer Rayleigh range, therefore exhibiting higher heralding efficiencies, following the proposed behaviour of ξ within Ref. [96].

laser, tuneable negative group velocity dispersion is introduced via a Gires–Tournois interferometer, allowing the user to fine tune the output pulse duration of the laser.

In order to generate PDC photons, we focus our pump beam into the centre of the crystal with a focusing lens that has a nominal 40 cm focusing length, generating a slightly elliptical spot with a waist of $\sim 124\mu\text{m}$ in the horizontal and $\sim 119\mu\text{m}$ in the vertical axis. This focusing condition was chosen as an optimal trade-off between brightness and heralding efficiency [96, 97, 103]. Empirically, we verified that a looser focusing condition increased the heralding efficiency, whilst resulted in a reduction in pair generation rate, following the conclusions drawn from Section 3.1.4, see Figure (3.4). From these results, we can obtain the values for average heralding and brightness, displayed in Table 3.1.

To collect the down-converted modes we separate the emitted photon pairs on a polarising beam splitter, with an initial dichroic mirror removing pump photons. Signal and idler photons are collected into single-mode fibres after long-pass filtering

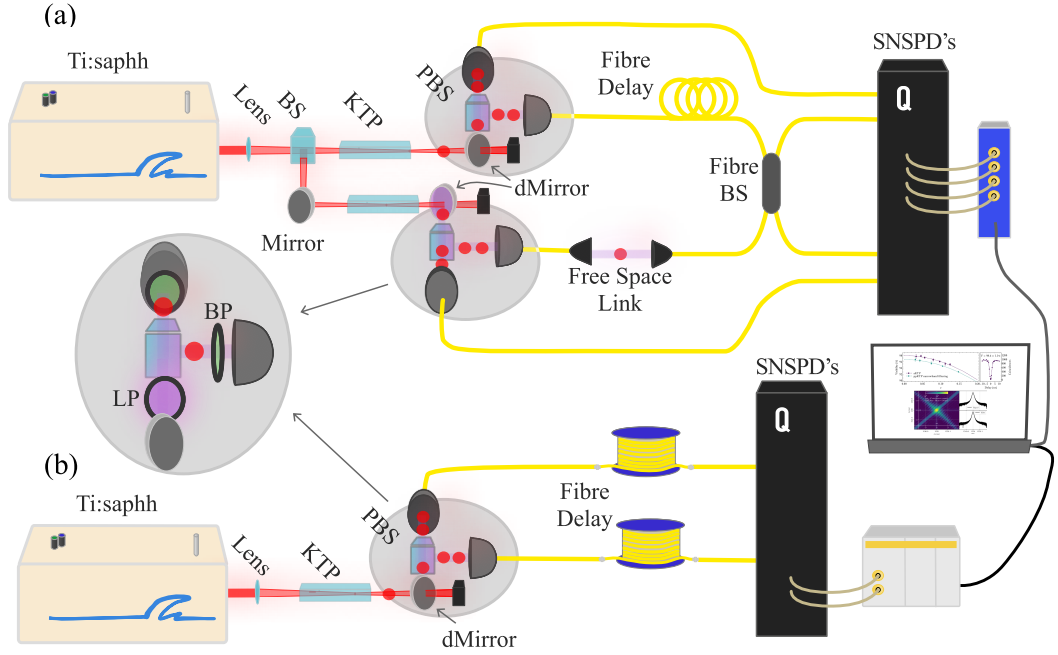


Figure 3.5: Experimental layout. (a) A Ti:Saphh laser pumps a standard ppKTP, or domain-engineered aKTP crystal, at a repetition rate of 80.9MHz. The down-converted photon pairs are collected after reflection from a dichroic mirror and separated by a PBS. Individual photons from two sources are temporally synchronised with an adjustable free-space gap before they are superposed in an in-fibre BS. Photons are then detected by Superconducting Nano-wire Single Photon Detectors (SNSPDs), with photon arrival times being time-tagged and processed. (b) Two ~ 20 km fibre spools of telecommunication grade fibre are used for dispersive spectroscopy, exploiting chromatic dispersion allowing us to reconstruct the joint photon spectrum [104]. We collect the photon pairs in the same manner as above, however the collected photons are subjected to the fibre delay.

to reduce any residual pump photons further. We introduce either some gentle filtering around the central spectral lobe of our down-converted photons—via a filter with a transmission profile of $\exp[-\frac{(\omega-\omega_0)^4}{2\sigma^4}]$ a FWHM of 7.4 nm and is ~ 5 times wider than the generated photon bandwidth which minimally impacts heralding efficiencies—or tight filtering depending on the type of KTP crystal being analysed. The profile of these filters are shown in Figure 3.6. Down-converted photons then pass through optical interference or spectroscopy setups before being collected by SNSPDs operating at $\sim 80\%$ detection efficiencies. See Figure (3.5) (a) and (b) for the experimental arrangements.

3.2.2 Independent Hong-Ou-Mandel

As previously stated, we investigated two-photon interference visibilities for different configurations of crystals—a 22 mm ppKTP crystal and a 30 mm custom-poled

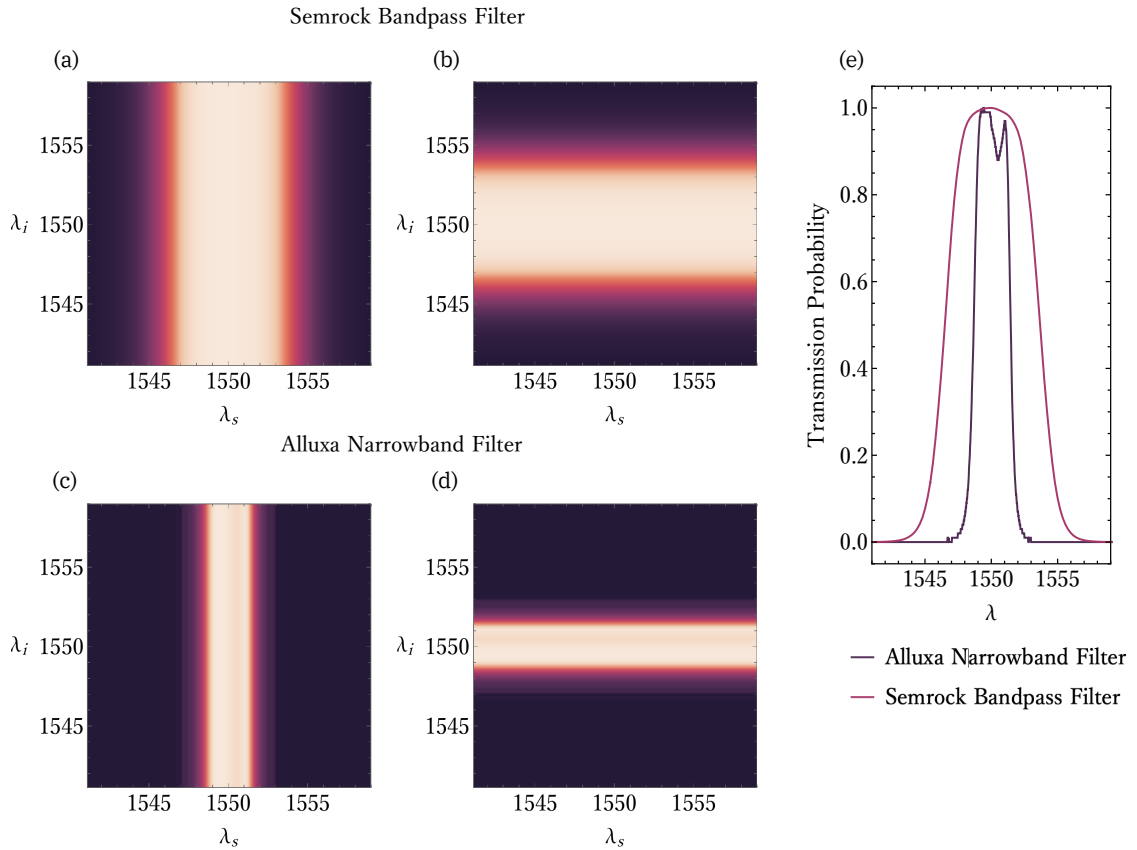


Figure 3.6: Spectral bandwidth of filters used in source investigation. The filters we use for the aKTP crystals in the signal mode (a) and idler mode (b), and ppKTP crystals in the signal modes (c) and idler modes (d). We also show a more intuitive figure for directly comparing the bandwidths of the two filters (e). From these figures we can see that the Alluxa filters are much narrower, ≤ 3 nm, compared to the 7.4 nm FWHM of the Semrock bandpass filter. The Alluxa filters were selected for their ability to filter out just the central lobe of the joint photon spectrum of the ppKTP crystals, thus increasing the spectral purity, but also impinging loss onto each of the down-converted modes.

aKTP crystal—and filters. We interfered photons generated from separate, but identical (manufactured from the same lithographic mask) crystals. In order to obtain a lower bound on the implied photon purity and to generate the data in Figure 3.7 (a), the two sources were pumped with the same amount of pump power, for a variety of different pump powers, and at least five independent two-photon interference scans were run consecutively. The data acquisition time for each of these scans was sufficient to obtain at least 1000 four-photon coincidence events outside of the dip position. In order to find the appropriate data acquisition time, the linear stage that controls the amount temporal delay applied to one of the photons, was shifted to well outside the position of interference, and photon detection statistics were gathered, determining the photon generation rate and therefore the required acquisition time. From the final data set, containing pump power and respective in-

interference visibilities, we fit a linear function and extrapolate the expected visibility at zero pump power. This technique eliminates visibility degradation due to photon-number impurity (see the Appendix of Ref. [90]) and serves to lower bound photon purity. The performance of all results are summarised in Table 3.1. Importantly, the generation rates and heralding efficiencies are quoted with consistent focusing conditions in the same optical setup and provide a comparison and not an upper limit on crystal performances. Different pump focusing conditions as well as different collection optics will result in different values for source brightness, heralding efficiencies and can also impact photon purity [96].

We observe an improvement in both interference visibility and generation rates upon Ref. [90], a result of altering the width of the Gaussian target function tracked by our algorithm from $\sigma = l/4$ to $\sigma = l/4.7$. Ref. [90] reported a lower bound purity of $92.7 \pm 0.2\%$. This data was obtained using a delayed two-photon interference technique, interfering photons generated from the same source separated, delayed by a time that is an integer value of laser repetition rates. Instead of using this technique again, we perform interference measurements on photons from independent crystals, representing a true proxy for source scalability. Our new apodized crystals have a lower-bound purity, under the same gentle filtering, of $98.0 \pm 0.1\%$. Without any filtering we obtain a lower-bound purity of $95.3 \pm 0.1\%$ and the respective data contributes to a full plot of all results found in Figure 3.7.

Rather than expressing results in terms of pumping power, we show the main results in terms of γ , the effective squeezing of the two-mode squeezed vacuum, which encompasses the pump power and focusing conditions applied to the crystal. As we have seen, in the photon number basis n , the PDC process can be expressed as:

$$(1 - \gamma^2)^{1/2} \sum_{n=0}^{\infty} \gamma^n |n, n\rangle_{s,i},$$

with γ defined as: $\gamma = (\tau P)^{1/2}$, where now P is the average pump power and τ is a constant quantifying the non-linear interaction of the medium. This was explored back in Section 2.3.1, so for obtaining the parameter γ we address the readers attention back to there. We evaluate γ from the measured coincidence rates, single rates and the clock rate of the pulsed laser. With knowledge of γ , the photon pair rate and multi-photon pair rates can be determined. This forms a more representative analysis of crystal performance as the variety of experimental

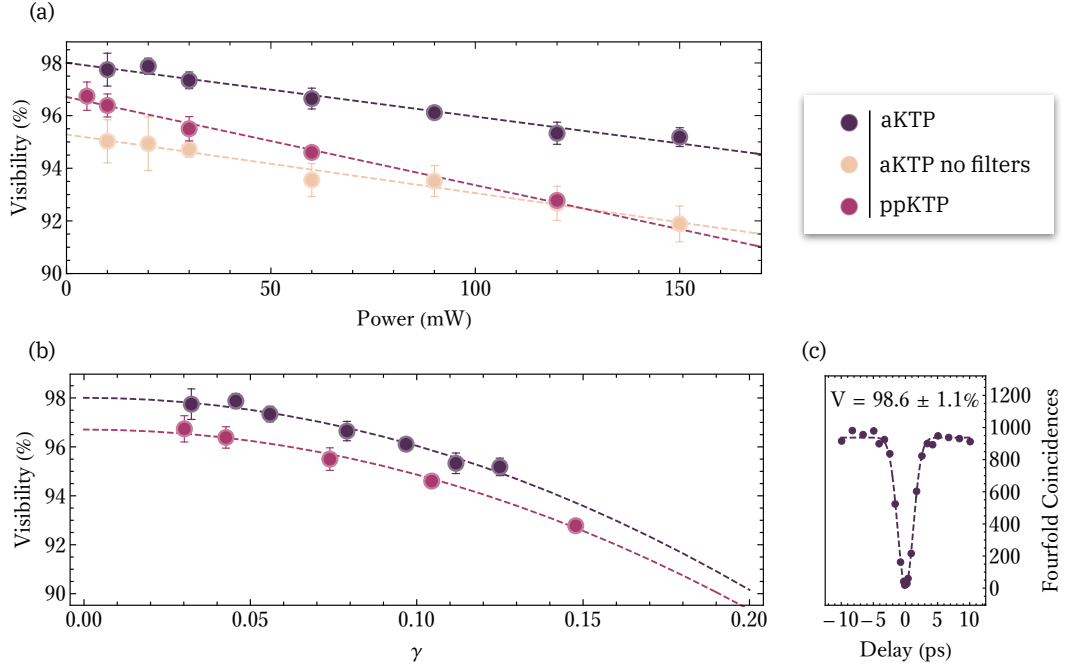


Figure 3.7: Experimental results for the visibility of two-photon interference. (a) Interference visibilities dependence on pump power and (b) visibility dependence on the squeezing parameter, γ . Each data point represents the average visibility from five interference measurements for each value of pump power (or, equivalently, for each value of γ). From this data set we can infer a minimum spectral purity of $98.0 \pm 0.1\%$ and compare the performance of our aKTP crystals with loose spectral filtering against a ppKTP crystal with narrow-band, tight spectral filtering. (c) A two-photon interference measurement between photons generated from separate sources. At a pump power of 10 mW we achieve an interference visibility of $98.6 \pm 1.1\%$, with a four-photon coincidence rate of around 5 Hz.

conditions distinct to our analysis are gathered into this one term, lending this work to be more repeatable. Figure (3.7) (b) compares the interference visibility of our aKTP crystals performance with a ppKTP crystal as a function the squeezing γ .

With apodization, the need for tight filtering is removed, resulting in significantly higher heralding efficiencies, seen in Table 3.1. This higher efficiency means that when both sources are generating photons at the same raw rate, the source with higher heralding efficiencies will lead to higher rates of detector clicks. Factoring out known optical losses and detection efficiencies (taken as the quoted operational upper bound of 80%), overall collection efficiencies are lower bounded to 91.8%. Optical losses were determined by measuring the transmission properties of each optical element between pair production and the housing of our detectors, this accounted for a loss of 7.9%. Anti-reflection coated optics were used where possible to minimise any losses, including on the end facets of all the KTP crystals used in this investigation.

Crystal	Interference Visibility (%)	Mean Heralding Efficiency (%)	Collection Efficiency (%)	Mean Brightness (cc/mW/s)	Experimental $\sqrt{\text{JSI}}$ Purity (%)	Theoretical JSA Purity (%)
aKTP	98.0 ± 0.1	67.5	91.8	3900	91.17 ± 0.02	98.7
ppKTP	95.3 ± 0.1	57.2	77.4	4900	94.43 ± 0.03	98.4

Table 3.1: A summary of results comparing our custom aKTP crystal with loose spectral filters to a ppKTP crystal with tight spectral filters. The interference visibilities are quoted at zero pump power. The mean heralding efficiencies and brightness respectively for each crystal result from an analysis of the performance of each source as a function of pump power. The collection efficiencies are calculated with respect to the upper limit detection efficiency of our detectors (80%) as well as other known optical losses (7.9%). Finally we also include the purities calculated from our experimental JSI reconstructions, as well as the theoretical purities. We use the $\sqrt{\text{JSI}}$ to calculate purities as it represents a better approximation of the JSA compared to calculating the purity of the JSI [69].

3.2.3 Reconstructing the Joint Spectrum

Another means of quantifying source performance is to analyse a reconstruction of the joint photon spectrum. Reconstruction of the JSA is experimentally demanding since it requires a spectrally resolved amplitude and phase measurement, which can be achieved for example via phase-sensitive stimulated emission tomography [105]. Constructing the joint spectral intensity (JSI), equivalent to $|\text{JSA}|^2$, can be achieved with comparative ease and is therefore commonly shown, although one has to be careful what conclusions to draw in the absence of phase information normally contained in the JSA [69]. With 20 km of standard telecommunication fibre optic we can exploit chromatic dispersion to map photon arrival time to the associated spectral component of the JSI, as performed in [94]. The experimental arrangement is depicted in Figure (3.5) (b). Collection of at least 10^6 photons detected by SNSPD's operating with < 50 ps jitter, < 25 ns reset time and processed via a Picoquant HydraHarp with 1 ps timing resolution, enabled the construction of the respective JSI for combinations of filter and crystal. The spectral window of our results span 12.5 ns and the achievable timing resolution of this spectrometer translates to a spatial resolution of ~ 0.0028 nm. Figure (3.8) (a), (b) and (c), (d) show the respective experimental JSIs of un-filtered aKTP and un-filtered ppKTP, with and without a logarithmic scale respectively. Any spectral correlations that exist along the main diagonal are visually highlighted. These correlation are clearly prevalent for ppKTP but almost non-existent for unfiltered aKTP, a result of non-zero contributions from

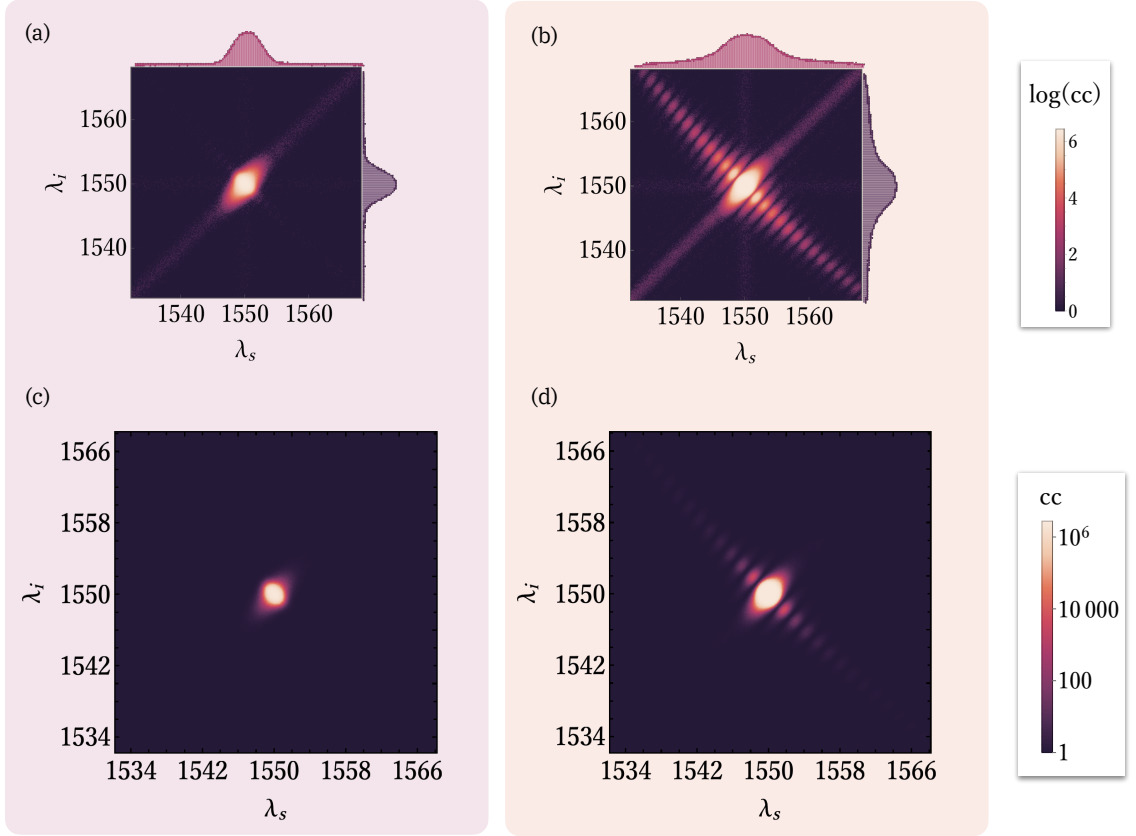


Figure 3.8: Reconstruction of the JSI. Experimental reconstructions of the JSI (and marginal photon spectrum for (a) and (b)). Using a dispersive spectroscopy technique, we construct the full joint spectrum spanning a whole repetition of our lasers cycle, for our aKTP crystal (a), (c) and ppKTP crystal (b), (d). The reconstruction reveals all spectral correlations which are then either suppressed by filtering, or already suppressed through modification of the PMF. Using a logarithmic scale (a) and (b), we can visually highlight any prevalent correlations. These correlation are much more noticeable for the ppKTP crystal, enforcing the need to filter out these purity degrading correlations in order to achieve high interference visibilities.

the PMF. Along the diagonal, from bottom left to the top right, as well parallel to the x and y axes, through the central lobe of the joint spectra, we see a constant background signal arising from dark counts. An additional PDC source was used as a trigger, to measure the arrival of signal and idler photons. A dark count detected in the trigger channel, as opposed to an actual photon, corresponds to a displacement of the central lobe along the diagonal, resulting in temporally correlated background noise. If, either the signal or idler photon is lost, but a dark count is detected in that channel along with the trigger and remaining signal/idler photon, the central lobe is shifted in the parallel to the x or y axes depending on which of signal and idler photons are lost. The probability of this is smaller, proportional to the pair emission probability.

To produce estimates for both the JSI and $\sqrt{\text{JSI}}$ purities, we reconstructed the

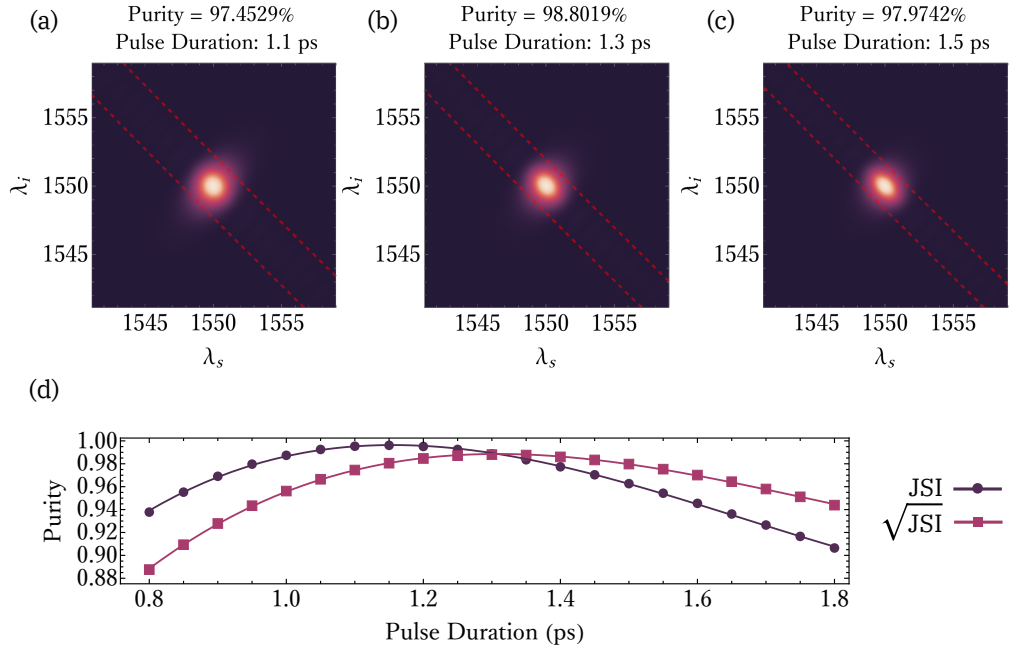


Figure 3.9: Theoretical simulations of photon purity as a function of varying pulse duration. A non-ideal pulse duration affects photon purity as the bandwidths of the PEF and PMF are not matched for pulse durations not 1.3 ps. (a), (b) and (c) depict the JSI from a range of pulse durations. Shorter pulse durations contribute towards spectral correlations along the diagonal, something visible in our reconstructed $\sqrt{\text{JSI}}$ s. The red dash lines represent the width of the PEF corresponding to the pulse duration under investigation. (d) The effects of non-ideal pulse durations on photon purity. Analysing the range of purities derived from $\sqrt{\text{JSI}}$ and JSI as a function of pump pulse duration.

JSI across increasingly long measurement intervals. Each estimation is calculated using 50×50 ps bins; doing so reduces the sparsity of the raw data and provides a more accurate and reliable Singular Value Decomposition (SVD). The SVD is used to numerically implement the Schmidt decomposition, used to quantify the non-separability of the JSA [74]. By observing the value the estimation converges towards, we truncate the total measurement time to avoid instability. These estimation of purities are contained in Table 3.1. Neither the JSI nor the $\sqrt{\text{JSI}}$ truly reveal photon purity due to lack of phase information, something two-photon interference can incorporate [69]. Thus, two-photon interference results represent a more faithful estimate of photon purity. Discrepancies between the lower-bound purities determined by two-photon interference results, and inferred purities from experimental JSIs could be caused by a combination of different factors, such as drifts in the laser central frequency and pulse duration, as well as non-negligible jitter in the detection system. Visually noticeable elongation of central lobe along the diagonal suggests pump pulse durations that are shorter than the crystal is optimised for, which in turn would result in a lower purity for experimental JSI analysis.

3.2.3.1 Elongation of Joint Spectrum

Our efforts to consider why we witnessed lower purities in our experimental JSI analysis led to simulations into how pulse duration affects photon purity, the results of which are shown in Figure (3.9). Maximum purities are achieved when the width of the PEF and PMF are matched [69]. From the JSI reconstruction results, the elongation along the diagonal could have been caused by instability of our pulsed laser source, a reasonable argument as scans were run for hours at a time. Any drifting in pulse duration from ideal leads to a reduction in purity. From simulations we estimate that, pulse durations that are ± 0.4 ps away from the ideal value can result in purities dropping by 6%. This simulation calculates the resulting JSA from the PMF and the PEF of various widths dictated by an array of different pulse durations of the pump.

3.3 Concluding remarks

The importance of achieving the photon source characteristics displayed in this chapter was recently highlighted in Ref. [106], which concludes that quantum supremacy in a Boson sampling task with non-multiplexed single-photons from PDC sources can only be achieved with Gaussian-profile aKTP crystals due to the higher collection efficiencies. Notably, photonic quantum supremacy has just been demonstrated in Gaussian Boson Sampling (GBS), in an experiment which created 50 photons from 25 Gaussian apodized crystals using a duty-cycle poling technique [34]. Using our

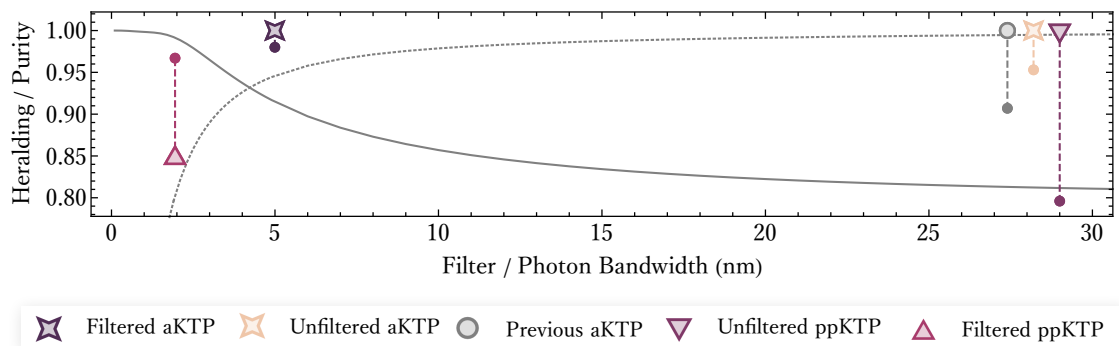


Figure 3.10: Filter bandwidth and effects on purity and heralding. Normalised heralding and purities of the crystals we have analysed in this manuscript as a function of the photon bandwidth or the filtered photon bandwidth. The solid data points represent the normalised purity, the filled alternating shaped data points are heralding values. The solid (dashed) lines are the simulated results of the purity (heralding) for the ppKTP crystal.

improved poling algorithm and considering the trade off between non-linearity and photon purity highlighted in this manuscript, an optimal σ could enable higher purities and heralding efficiencies. This, in turn, would culminate in a greater advantage and scalability of the scheme.

The discrepancy in brightness between our aKTP source and the ppKTP source highlighted within Table 3.1 can be balanced by adjusting the relative pump powers to achieve the same squeezing γ . At a fixed value of γ , the single and multi-pair production probability for aKTP and ppKTP are the same, independent of the pump power, as the different pumping powers act to equate the probabilities of generating n photon pairs. A hard limit on available pump power for multiple bulk PDC sources could restrict one's ability to maximise brightness. Future scalable architectures however are likely to be based on waveguides, which typically require only μW of pumping power. Gaussian PMFs can also be achieved in waveguide sources either through domain engineering, or via inter-modal Spontaneous Four Wave Mixing (SFWM) in a multi-mode waveguide [107].

Future improvements to target higher interference visibilities could be achieved through modifying the PEF. Currently, the PEF is a 1.3 ps long sech^2 pulse optimised for crystal length and thus PMF width, imposing a theoretical limit on the maximum visibility of 98.7%. However, it is possible to achieve up to 99.9% visibility directly with our crystals by engineering the PEF [69]. Modification of the PEF can be achieved using pump-shaping techniques [85]. Additionally, incremental improvements can be made with a deeper exploration into the interplay of spatial and spectral modes generated in a non-linearity engineered crystals [108, 109].

3.3.1 Acknowledgements

This work built upon previous work conducted by Francesco Graffitti. He also aided in the performing the experiment work as well as the analysis contained here. Peter Barrow also contributed to the analysis, whilst Christopher L. Morrison and Joseph Ho provided help with this work with fruitful discussions. Agata G. Brańczyk and Alessandro Federizzi conceived the project.

Chapter 4

Generating Multi-partite Entanglement

4.1	Entangled photon sources	68
4.1.1	Sagnac interferometer	69
4.1.1.1	Note on optical alignment	72
4.2	Linear optical fusion gates	73
4.2.1	Type-I fusion gate	74
4.2.2	Type-II fusion gate	74
4.2.3	Fusion transformations	76
4.2.4	Operating linear optical fusion gates	77
4.3	Concluding remarks	79

This chapter acts as a short interlude between PDC source design and the generation of two-photon and multi-photon entanglement. PDC has been used extensively to generate entangled states for a huge variety of use cases, to say the reference list is extensive is an understatement, however a variety of them are presented in the following Refs. [31, 33, 110–118]. This chapter foremost discusses the generation of a Bell state and how we use custom designed optomechanics to generate this. We then discuss methods to generate larger entangled states that depend on two-photon interference. Achieving two-photon interference with high success probability encountering minimal errors high interference visibility is an absolute prerequisite for this interaction to occur efficiently, something that has been an underlying narrative throughout this thesis so far and will continue to be in the following final chapters. The generation of multi-partite entangled states depends on non-local gates that require the interaction of two indistinguishable photons. Using our custom crystals gives us an inherent advantage over other sources by maximising heralding efficiencies and achieving as close to unit photon purities as possible, two parameters that are intrinsic to efficiently generating larger states via two-photon interference.

4.1 Entangled photon sources

The first use of PDC to generate an entangled state was proposed and shown by Kwiat *et al.* in Ref. [23]. In Kwiat’s work, the non-collinearity of bulk PDC was exploited, and when collecting photons at the intercept of the emission cones of the PDC photons, an entangled state was created due to the indistinguishability of which cone each collected photon was from. The rather large caveat to this technique however was loss. Photons are generated across all points on the emission cones, so collecting photon on the intercept of both cones only—in order to make sure state quality is good—meant that all other photons were lost. The first use of an interferometric scheme was introduced in [119], after its proposal in [120], overcoming the large amount of loss and bidirectionally pumping a single KTP crystal. The lack of stability made this scheme sensitive to environmental perturbations—inspiring the idea of using a Sagnac interferometer in-stead of a folded Mach-Zender—which has all the benefits the bidirectional pumped interferometric scheme offers with additional robustness. Ultimately it was Kim *et al.* who combined the phase stable

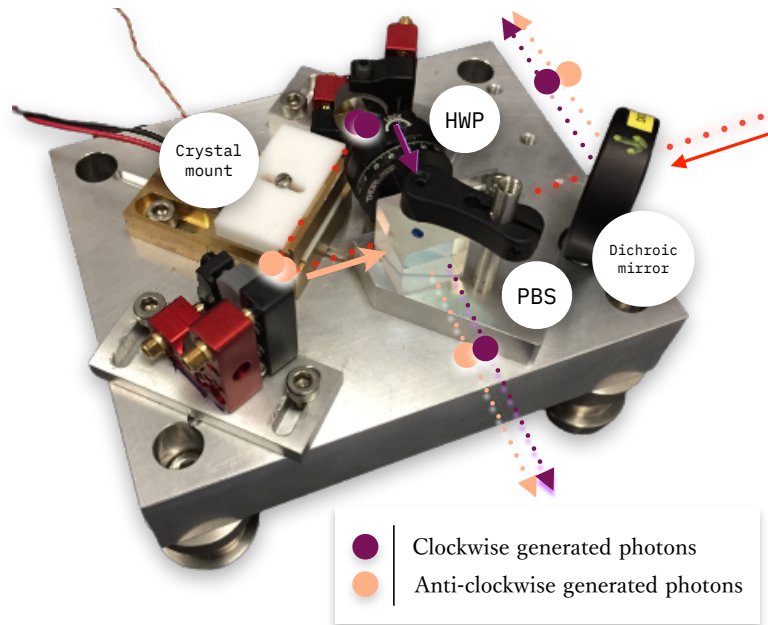


Figure 4.1: Building block for generating an entangled state. PDC occurs co-linearly and bi-directionally when a QPM PDC crystal is placed inside a sagnac interferometric scheme. The pump in our case is centred at 775nm and enters the sagnac by transmitting through a dichroic mirror which only reflects 1550nm. When the polarisation of the pump is aligned diagonally, equal superposition of the pump exits the PBS and produces PDC photons in either the clockwise direction or the anti-clockwise direction. This is enabled by the presence of a HWP inside the sagnac loop, that rotates V polarised photons from the reflection port of the PBS to H polarisation, making sure that the type-II PDC process takes place. The crystal is contained in a temperature controllable mount in order to make shifts to the phase mismatch and enable degenerate PDC photons. PDC photon pairs (pink for anti-clockwise and purple for clockwise) then propagate around the sagnac and are separated based on their orthogonality in polarisation on the PBS. In one output mode of the PBS for each pump direction, the beam overlaps with the pump. In this case the dichroic mirror reflects the PDC photons for collection into a single-mode fibre. The remaining output mode of the PBS is also collected into a single-mode fibre.

interferometry with a bidirectionally pumped ppKTP source of photons [121]. Fine tuning this setup, Fedrizzi *et al.* in Ref [122] delivered what is effectively the first iteration of the scheme for generating entangled photons we present in the following, and used extensively within the bulk PDC community.

4.1.1 Sagnac interferometer

A Sagnac interferometer consists of two mirrors and a PBS. Figure (4.1) depicts the optical arrangement. A diagonally polarised pump photon is prepared and subsequently sent into this interferometer. It passes through a dichroic mirror which only reflects photons centred around the down-conversion wavelengths. This pump

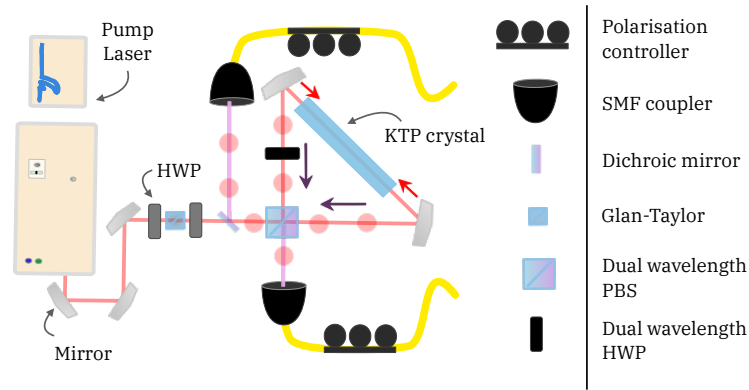


Figure 4.2: Schematic for entanglement generation with PDC using a Sagnac interferometer. A pair of entangled photons can be generated from PDC when the non-linear media is placed inside an interferometer. The pump photon either generates a photon pair in the clockwise and anti-clockwise direction. Its polarisation is prepared with a HWP after a Glan-Taylor (GT) which ensures polarisation is set to the linear basis. The amount of power into the source is controlled by an additional HWP in front of the GT. Once photons are generated, they are collected into single-mode fibres (SMFs).

photon is then split by a PBS into its basis polarisation components H and V . The reflected V component of the photon is then rotated to H by a dual wavelength HWP, such that the crystal is pumped in both directions by a horizontally polarised field, allowing bi-directional type-II PDC. The photons generated in type-II PDC are orthogonal in polarisation, and propagate around the interferometer in clockwise and anti-clockwise directions.

This optical arrangement offers compensation for the longitudinal walk off that emanates from the different propagation velocities (property of birefringence) of each photon inside the non-linear crystal. Rather than compensating for this walk off with (relatively) complicated techniques involving the use of another birefringent wedge in one of the arms¹, the dual wavelength HWP inside the Sagnac loop maintains quality entanglement by preventing the temporal discrepancies and maintaining photon coherence. The walk off is not fully eradicated, but the HWPs retardation re-maps the polarisation states of one the down-converted photon pairs propagating in one direction whilst the other pair is not subjected to any retardations, minimising the delay after the PBS. Once at the PBS, both pairs of photons are split such that we get a H photon from one pair production and a V photon from the other pair production in each collection mode. Thus, in one collection mode you could have either $|H_s\rangle_1$ or $|V_i\rangle_2$ arriving, whilst arriving at the other mode you would have

¹These techniques can also introduce photon loss, something we absolutely want to avoid.

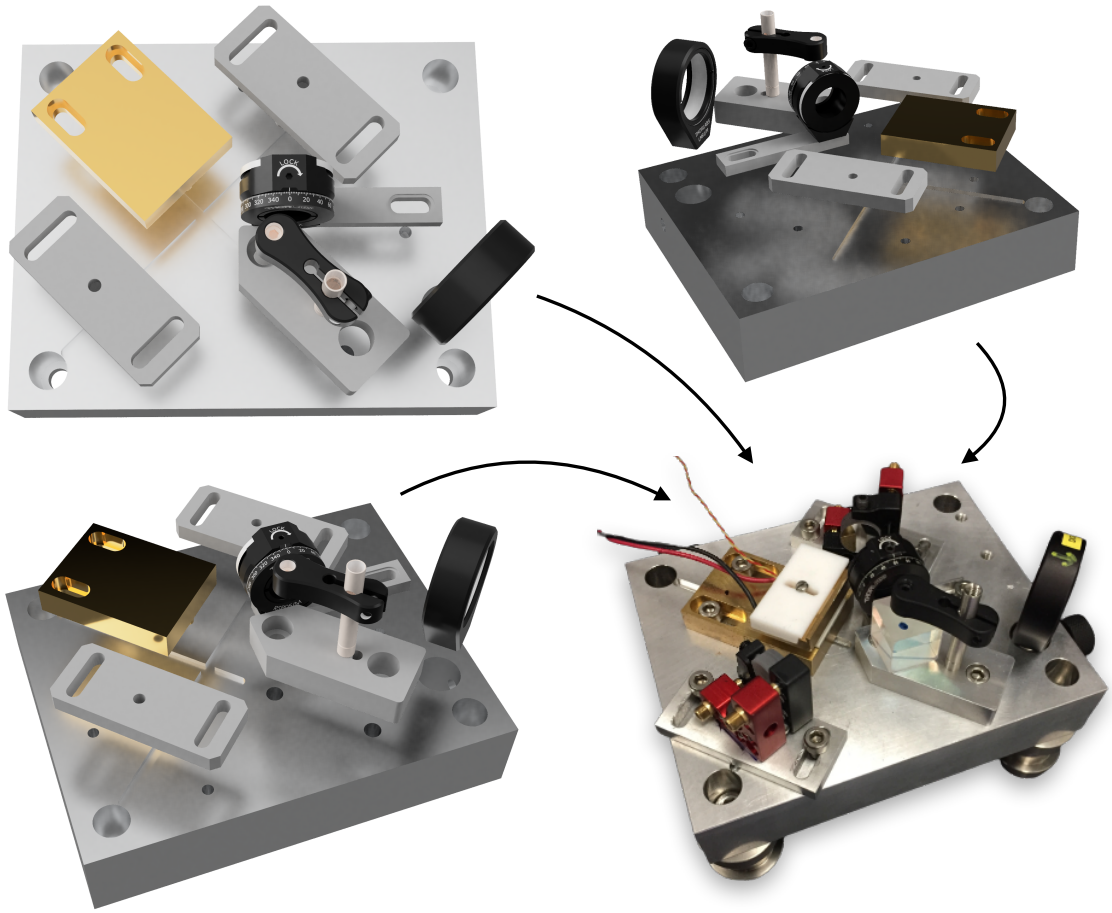


Figure 4.3: Design for a module compact source and the final outcome. The idea for employing a notch and groove system comes from fibre coupling systems, where typically one wants to restrict the degrees of freedom the fibre tip possesses in order to make it easier to optimise the optical alignment. Like in the case for fibre coupling, the initial alignment of the input beam is crucial, as without ideal initial alignment, the restriction to degrees of freedom means that any initial miss-alignment cannot be corrected for. The base module is 100mm by 125mm, and contains the dichroic mirror, HWP, PBS, two mirrors, the crystal and its temperature controllable mount.

either $|H_s\rangle_2$ or $|V_i\rangle_1$. You cannot know which photons are arriving in each collection mode, as you have no knowledge about which photon pair was created, a feature of the pump being aligned to an equal superposition of H and V. Your output quantum state is therefore,

$$|\Psi\rangle^\pm = \frac{1}{\sqrt{2}}(|H_s\rangle |V_i\rangle + e^{i\phi} |V_s\rangle |H_i\rangle) \quad (4.1)$$

where the term ϕ exists as a result of the phase difference between the components of the pump field and any phases picked up by the down-converted photons in the Sagnac loop. This is a maximally entangled Bell state, locally equivalent to the other three Bell states, and is the resource state for our investigations into QIP tasks.

4.1.1.1 Note on optical alignment

Aligning this interferometer is tricky, but there are some things which we implemented into the design of the interferometer that restrict the degrees of freedom making the alignment a little easier. Rather than using bulk optical components sitting on individual pillars, we made a choice to create a single block which contain most of the optical components critical for the correct alignment. There are several benefits to this approach but also a few disadvantages. Addressing the downfalls first, the restriction on the angle of the PBS means we cannot exploit the optimal angle of incidence of a PBS. Obtaining a higher extinction ratio in the transmis-

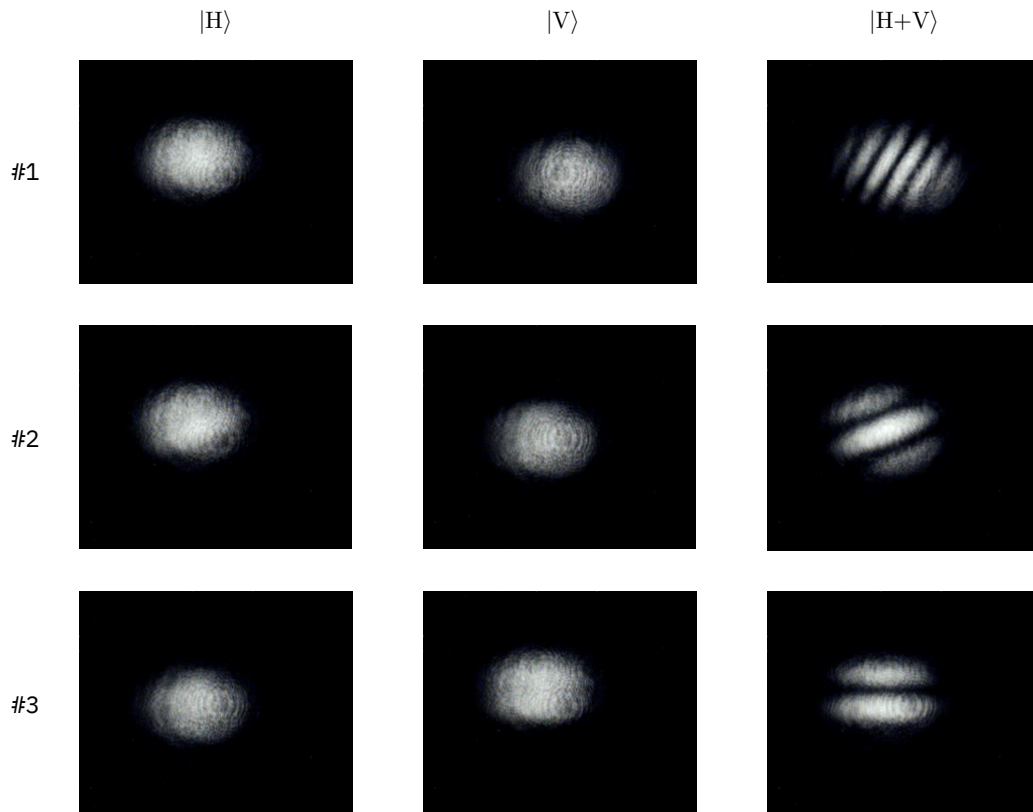


Figure 4.4: Alignment of the Sagnac interferometer. Each row of images shows the iteration of trying to overlap the two paths of the Sagnac interferometer. The first and second column of figures are images taken of the pump after propagating around either the clockwise direction, where the pump polarisation was $|H\rangle$, or in the anti-clockwise direction, where the pump polarisation was $|V\rangle$. A neat trick is to use a linear plate polariser in front of a camera, and rotate the polariser to $|D\rangle$. This then images classical interference fringes that result from the overlap of the pump propagating in both directions and the subsequent constructive and destructive interference. In the first row, the overlap of the two paths is worse than the overlap than the last row, epitomised by the spacing and size of the destructive and constructive elements of the interference pattern. When the interference fringes take the form of a single spot—where the fringes are no longer visible—there is maximal overlap of the clockwise and anti-clockwise paths.

sion and reflection ports of the PBS is crucial for maximising the two-photon state purity, as any any bit errors in the computational (\mathbb{Z}) basis caused by the PBS creates mixture and reduces the purity of the entangled state. The benefits of such a design is firstly, the compactness of the final setup, meaning if one wants the place coupling optics as close to the source as possible for higher photon pair generation rates, then this can be achieved. Another benefit is the restriction to the degrees of freedom. Whilst this might sound slightly counter-intuitive, the nature of the way we align the sagnac—the beam path defining a right-angled triangle—means that there is a fixed geometry to the system reducing the number of steps we have to take in order to make sure the optics are placed in the correct positions. The mirror placement and tilt angle are fixed for achieving perfect alignment. To achieve this we borrowed a notch and groove system similar to the ones employed in fibre coupling modules, to constrict the components position, making the tedious full alignment process a lot easier. A full outline on how to align a sagnac interferometer for the purpose of generating entangled states with PDC—that is very in-depth and worth reading if you want to build this source—can be found in the appendix of Ref. [123]. Figure (4.3) shows the base containing the grooves as well as the the individual components which posses notches. Figure (4.4) depicts the alignment process.

We have discussed how to build a single Bell state, but to build larger states we need some additional optical arrangements.

4.2 Linear optical fusion gates

Linear optical fusion gates were first devised and introduced in Ref [124]. Their proposal lies at the foundation of a linear optical computing scheme that was less resource intensive and more efficient than those currently suggested [125, 126]. Instead of the more familiar CZ gates, a fusion gate was proposed.

These fusion gates are generalisations of two-photon HOM interference and synonymous with Bell state measurements. They take smaller entangled resource states (nominally Bell states) and produce larger entangled states. Effectively a projective entangling measure, these gates come in two forms.

4.2.1 Type-I fusion gate

Type-I fusion gates consist of two well defined spatial modes mixed onto a PBS as depicted in Figure (4.5)(a). On one of the two output spatial modes of the PBS, the polarisation state of the photon in this mode is rotated into the \mathbb{X} -basis via an optical element, for bulk linear optics this is typically a HWP. Then, in order to determine if the gate is successful at its operation, the now rotated photon is measured via polarisation discriminating detection. The fusion of two qubits into one qubit succeeds if and only if there is a single photon in each of the output modes of the PBS, the maximum probability that this can occur is $p = 1/2$ and only as a result of perfect two-photon interference (unit visibility), again further motivation for our custom KTP PDC sources. In circuit notation, this operation is the same as a CNOT gate between the two input logical qubits, followed by a measurement in the computational basis for the index matching that of the measured photon. The fusion will fail if this condition is not met, i.e. if there is photon bunching in one of the output modes of the PBS. This then become equivalent to a measurement in the \mathbb{Z} eigenbasis. Qubit fusion in the Type-I gate may succeed, but loss of the photon between this operation succeeding the the detection of the photon can lead to pauli errors going forward in linear optical quantum computing protocols [127], a drawback of this heralded gate.

4.2.2 Type-II fusion gate

Type-II fusion gates are an evolution of the Type-I gates. These evolved gates make use of redundant encoding in order to avoid some of the downfalls of the Type-I scheme. This is not to say that the Type-II fusion gate is better to implement, as their purpose should be considered on a case by case basis. Rather than destroying the logical qubits upon a failure, the Type-II gate implements a measurements on the \mathbb{X} eigenbasis on each of the input qubits. It operates in a very similar way to the Type-I fusion gate requiring two input qubits, but the subtlety here now is that both the input qubits and the output qubits are rotated into the \mathbb{X} eigenbasis and is only succesful upon post-selection (not a heralded gate). The successful operation of the fusion gate is effectively a projection onto the maximally entangled state $|\Phi^\pm\rangle$.

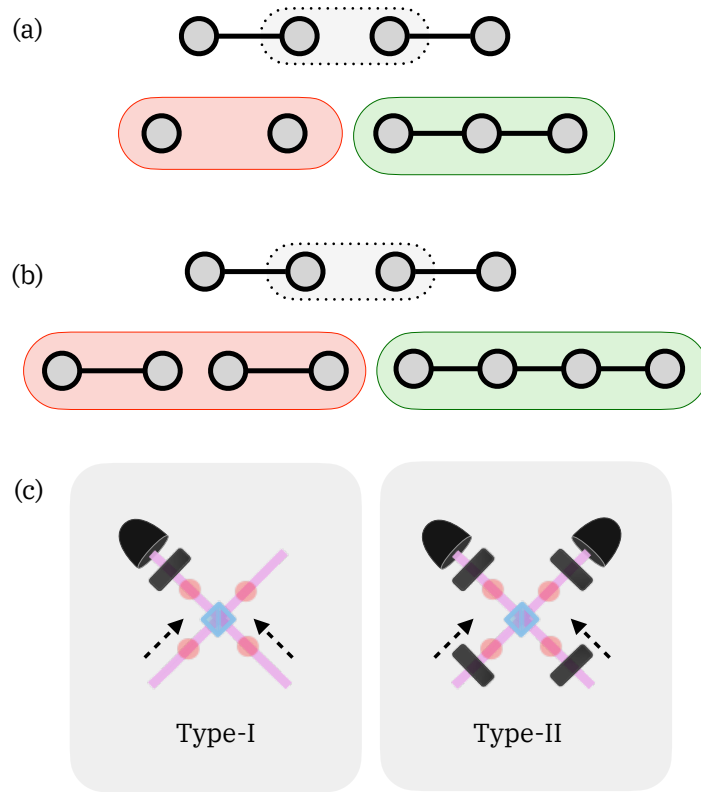


Figure 4.5: Fusion gates and their operation. The outcomes from success and failure of these gates are shown in (a) for the Type-I gate and (b) for Type-II. The success and failures are highlighted in green and red respectively. Notably, failure of the Type-II gate does not result in the destruction of input logical qubits, as until measurement, they are just rotated into the X eigenbasis. The optical arrangement for the two different kinds of linear optical fusion gates are displayed in (c).

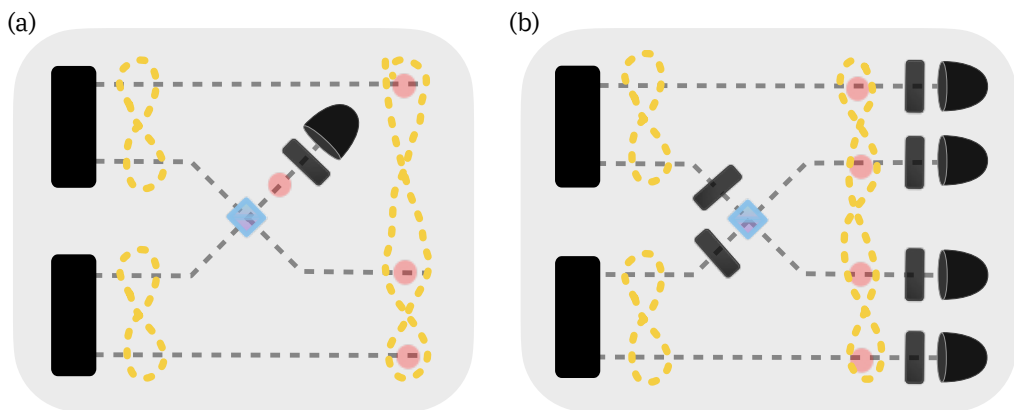


Figure 4.6: Fusion gates operating on well defined spatial modes. This figure defines what the typical optical layout of Type-I and Type-II fusion gates are, useful for visualising how the fusion gate transforms input states defined in specific spatial modes. For the Type-I gate (a), the un-measured photons in modes 1, 3 and 4 are transformed into a GHZ state. The GHZ states presence is heralded by the fusion. For the Type-II gate (b), there is no heralding and only post-selection on a photon in each mode results in the initial state being successfully transformed into a GHZ state between the modes.

4.2.3 Fusion transformations

Finally, now that we have defined the basic operation of both types of fusion gate, we can be a bit more succinct in their exact transformations by considering that the input photons for both gate types, are each bi-partitions of the maximally entangled Bell state $|\Phi^+\rangle$. Let us say that spatial modes 1 and 2 contain one Bell state $|\Phi^+\rangle_{12}$ and spatial modes 3 and 4 contain the other $|\Phi^+\rangle_{34}$, meaning a bi-partition of each state is held in the input modes of a PBS, spatial modes 2 and 3. Refer to Figure (4.6) for the schematic layout. For Type-I fusion, where an output photon is detected directly after the PBS, heralding the success of this gate, the transformation can be calculated via the following:

$$|\Phi^+\rangle_{12} |\Phi^+\rangle_{34} \frac{1}{\sqrt{2}} (|H\rangle_2 \langle HH|_{23} + |V\rangle_2 \langle VV|_{23}). \quad (4.2)$$

Expanding the above leaves the remaining un-measured qubits defined as a maximally entangled GHZ state:

$$|\text{GHZ}\rangle_{134} = \frac{1}{\sqrt{2}} (|HHH\rangle_{134} + |VVV\rangle_{134}). \quad (4.3)$$

For Type-II fusion one of the output photons is not immediately measured. Post-selection makes this gate possible, meaning that in order for this gate to be successful, all four photons in each spacial mode must be detected. Using a similar calculation for the Type-I fusion gates transformation it can be shown that rather than obtaining a 3-qubit GHZ state, the Type-II gate will produce a 4-qubit GHZ state upon post-selection. Measuring the presence of a photon in each mode lets us write the transformation as,

$$|\Phi^+\rangle_{12} |\Phi^+\rangle_{34} \frac{1}{\sqrt{2}} (|H\rangle_2 |H\rangle_3 \langle HH|_{23} + |V\rangle_2 |V\rangle_3 \langle VV|_{23}), \quad (4.4)$$

where now we arrive at a four-qubit GHZ state defined as,

$$|\text{GHZ}\rangle_{1234} = \frac{1}{\sqrt{2}} (|HHHH\rangle_{1234} + |VVVV\rangle_{1234}). \quad (4.5)$$

A neat property of fusion gates is their scalability. Although still operating with a maximum success probability of 1/2, fusion gates can be used successively and

with different input settings, an example of which will be shown in Chapter 5.

4.2.4 Operating linear optical fusion gates

In this subsection we outline how one operates fusion gates in practice, something crucial for obtaining and maintaining coherent multi-photon entangled states. When we discuss fusion gates and their operation in the experimental chapter following this one, the reader should refer back here in order to see how we set-up and ensure that the fusion gates are performing optimally.

In order for fusion gates to succeed with maximal probability, the input photons must be indistinguishable in their degrees of freedom, namely polarisation, temporal, spatial, spectral and photon number basis. Typically, the first step for realising these gates experimentally is to make sure there is suitable range for overlapping the wave-packets of each input photon in time, ideally with a motorised linear translation stage to do the precision work for you. Within the range of the translation stage one should be able to find perfect temporal overlap of the interfering photon wave-packets, corresponding to “sitting” in the HOM dip. This is an important first step in order make sure optimisation of other degrees of freedom is not in vain due a limited temporal range where the wave-packets are not temporally overlapped.

The spectral degree of freedom is fixed by the crystal, however it is always useful to check the sources and make sure they are at the required degenerate condition. This condition is met when the HOM visibility is maximal when interfering photons from the same PDC source.

We will assume that the spatial degree of freedom is correct as I am sure the experimenter reading this has aligned the fusion gate properly. Typically the best way to check this however is to overlap a classical diode source, split into two and sent into both arms of the fusion gate, on a camera in each output mode of the PBS.

Finally, for the polarisation degree of freedom there is a specific subtlety that is always prevalent in fusion gates employing bulk optics, this is the fact that the photons in the reflected port of the PBS pick up a phase. This phase is shown in Figure (4.7)(b) as the fringes are not centred at 0° . Using two QWPs orientated at 45° and a HWP sandwiched in-between, can correct this unwanted phase. By rotating the sandwiched HWP, the polarisation state of the qubit can be rotated around the X-Y plane of the Bloch sphere, correcting for any phase resulting mediated by

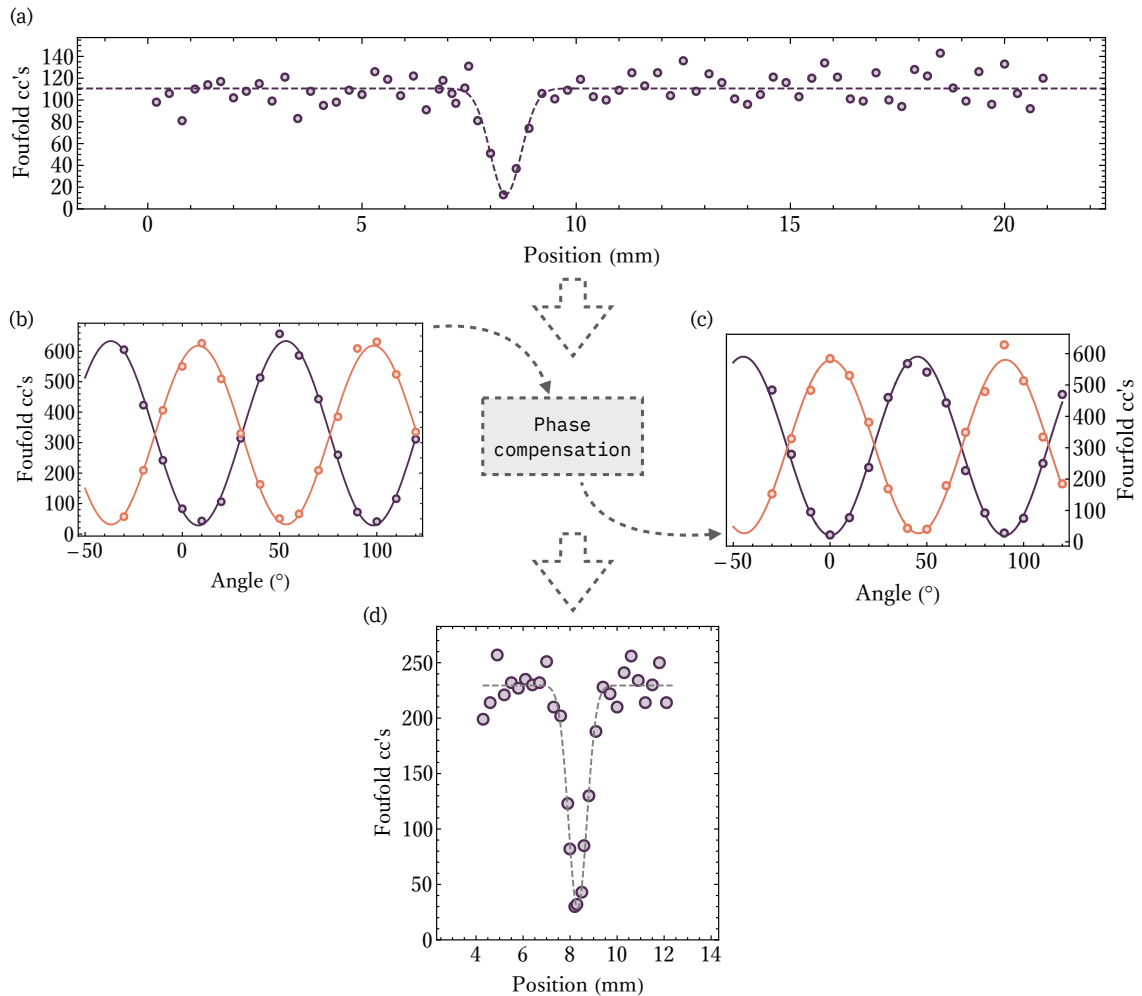


Figure 4.7: Preparing multi-photon states with linear optical fusions. Scanning a range, equivalent to implementing a positive or negative temporal delay to one of the photons undergoing two-photon interference, can reveal the zero temporal offset position. The plot (a) shows the HOM dip, and the zero temporal offset can be found via function fitting. Sitting in the minimum of the temporal dip, we can then determine if the correct polarisation states are prepared and if the spatial modes are overlapped. Improving the overlap and rotating the polarisation to increase the visibility of the interference corresponds to improving the probability of success of the fusion gate. Finally, implementing the correct phase compensation—shown in the plots (b) and (c)—then ensures that the purity of the GHZ state is maximal, correcting for the phase resulting from the PBS and from any phase discrepancy between the two input photons. Now, if phase compensation was correctly set, and all other degrees-of-freedom were optimised, then the resulting temporal interference scan (d) should provide a maximum visibility.

the interaction with the PBS. When using a fusion gate to create a GHZ state, this rotation does not effect population statistics in the \mathbb{Z} basis of the GHZ state, but does directly effect the \mathbb{X} basis and thus the coherence and purity of the effective GHZ state. Fixing the phase error results in a shift in the the interference fringes, see Figure (4.7) for how this looks.

Maintenance of the fusion gates is best achieved by checking the more accessible degrees of freedom of the photons. This includes checking that the polarisation state

of the incident photons has not changed, and if they have, re-optimize them with respect to the optical axes defined by the PBS upon which they interfere. Varying the delay one of the photon undergoes to ensure that the position is still in the HOM dip, and checking that the interference fringes are not shifted by re-checking the appropriate phase compensation is in place.

4.3 Concluding remarks

As we stated at the beginning of this chapter, the purpose was to bridge the gap between designing a photon and generating entanglement from that source. The chapter following this is a culmination of both the work in designing the PDC source as well as designing an optical arrangement which uses three fusion gates. Hence, it was important to include details on both how one generates Bell states, and also how one can use Bell states to generate larger states. Something we did not mention within this chapter but is important to consider, is if you are not operating in the symmetric GVM condition. Highlighted within Ref. [32], if you are not generating down-converted photons in the symmetric GVM condition, your JSA will not be circular, and which of the signal-idler photon pair enters the fusion gate should be carefully considered. For us, interfering signal photon with either a signal or idler photon generated from a different pair has negligible effects on interference visibilities, but this is not a universal case. Generally, consider only interfering only signal photons or only idler photons from the pair sources and craft the optical scheme with this in mind. For example, in the case of Ref. [32], the author only chose to interfere V photons.

Chapter 5

Photonic Graph States for Quantum Networks

5.1	Key distribution within a network	82
5.1.1	Quantum key distribution	82
5.1.2	Conference key agreement	84
5.1.2.1	Asymptotic key rate comparison	86
5.2	Experimental Network Communication	87
5.2.1	Generating an Optical Graph State	89
5.2.2	Transforming into an Optical Graph State	91
5.2.2.1	Distilling states	92
5.2.3	Experimental Preparation of State	95
5.2.4	Experimental verification of state	98
5.2.4.1	Flipped wave-plates	101
5.2.5	Obtaining desired state	103
5.2.5.1	LC operations	104
5.2.5.2	AKR	108
5.3	Concluding remarks	109
5.3.1	Acknowledgements	111

Lets propose that, in the not so distant future, there exists a quantum network. This network may consist of a blend of hybrid quantum architectures, but let us assume that any primitive network will contain basic quantum technologies; local operations and classical communication (LOCC), quantum channels and the ability to prepare and measure quantum states.

Specifically, for communicating within such a network, current proposals of quantum networks involve users sharing Bell states and performing “traditional” point-to-point quantum key distribution (QKD) protocols. This involves a user (Alice) designating who in the network they wish to communicate with (Bob), and sharing an entangled Bell state with them via entangled state creation and a sequence of entanglement swapping operations. Whilst there are many benefits to using this approach, like the generation of deterministic Bell states, favourable photon scaling and full finite key analysis, there are also some less trivial steps. Current near term proposals rely on routing algorithms to determine the most efficient route from Alice to Bob who need to be separated by channels with minimal loss, minimal noise, achieve sufficient entanglement distillation and to store quantum states in quantum memories located at network nodes.

It is without any question, wise to consider other proposals of how communication within a quantum network could look. Departing from the approach of using just Bell states as a quantum resource for point-to-point communication, we propose that a larger state acts as a global network resource state. In this scenario, we open up the possibility of not only performing 2-party QKD, but also N-party QKD, making use of recent experimental work on multi-user communication protocols [128]. Whats more, is that we can draw a direct comparison between a 2-party QKD approach and a N-party QKD approach due to the structure of the shared resource state and the ability to distill Bell pairs and GHZ states from it in a single network usage.

More explicitly, in the following chapter we outline a scheme involving 6 users each possessing a partition of a 6-photon graph state. From this resource state we can directly compare the rates at which a subset of the six users can communicate using either a 2-party QKD technique or a N-party QKD technique. We show that the key rate for an N-party QKD is at least a factor of two greater than that for 2-party QKD. This project is still on-going, and is a culmination of the design efforts put into PDC sources as well experimental techniques developed throughout my

Ph.D.

5.1 Key distribution within a network

Quantum key distribution in the past few decades has certainly bridged the gap between theoretical postulation and experimental realisation and is on the brink of full commercialisation. There have been numerous technological milestones and huge leaps in QKD, including fibre based QKD beyond repeater-less distances, free space QKD, QKD through sub-marine fibres and intercontinental QKD involving satellite links. The motivation of having secure communications is obvious, but one could argue that until we have the ability to perform useful quantum computations such as Shor’s algorithm [129], classical systems would suffice. But current classical crypto-systems, such as the Rivest-Shamir-Adleman protocol (RSA) [130], are also only secure due to the lack of an efficient algorithm. Whilst work is taking place trying to establish quantum safe crypto-systems [131], QKD remains the only realistic way to exchange information-theoretic secure keys, protected against adversaries with a quantum computer capable of universal computation.

In order to understand how a multi-user network could function is it useful to understand primitive key distribution protocols. A recent overview of quantum cryptography is found here in Ref. [132], whilst plenty more reviews exist in literature such as Refs. [133–135].

5.1.1 Quantum key distribution

The widely known “BB84” work is distinct from the “E91” protocol and, lying conceptually in-between these two protocols is “BBM92”. Within the BB84 protocol there are two users Alice and Bob, one the sender and one the receiver, linked via a quantum channel. The sender, let’s say Alice, has access to a source of photons and can prepare four different states belonging to two complementary bases, typically the Z basis and the X basis. The binary outcome 0 is ascribed to two of the non-orthogonal states $|H\rangle$ and $|D\rangle$, whilst the binary outcome 1 ascribed to $|V\rangle$ and $|A\rangle$. The non-orthogonality of these states ensures that any eavesdropper (Eve) cannot measure or clone the states with perfect fidelity [136]. The user who receives the states, Bob, performs measurements in either of the two bases. When Bob measures

in the same basis that Alice prepared the photon in, then they should both obtain the same bit value. If Bob does not measure in the same basis, then upon reconciling their bit values, the results will be random. These steps are repeated for a number of rounds, after which Alice and Bob stop the preparing and measuring of states and begin the classical procedure of sifting. The sifted key, contains all the binary elements of the initial key, but all of the occasions when Alice and Bob did not send and measure in the same bases are discarded. This step is performed over a classical channel. The final step to obtain the final secret key, is to select a subset of the sifted key to compare, if Alice and Bob agree on the outcomes of this subset, the bits are discarded and Alice and Bob are left with the final secret key. In the absence of noise and measurement errors, any disagreement in they key signifies the presence of Eve. Realistically, noise will always be present in a quantum channel, but we cannot distinguish between noise and the presence of Eve without sacrificing key security. To assume that Eve could not just simulate additional noise would be naive. It is therefore important to take the stance of a pessimist and assume that all errors resulting from noise are a result of the involvement of Eve. To avoid aborting the protocol altogether, Alice and Bob can perform an additional stage known as privacy amplification (PA) comprised of error correction algorithms and compression algorithms. In order to determine the amount of PA required, Alice and Bob need to determine the quantum bit error rate (QBER). If the QBER is above a certain threshold whereby no key could be generated, Alice and Bob will abort the protocol. Unconditional security of this protocol was shown in the simplest form by Shor and Preskill [137], simplifying the proofs of Refs. [138, 139]. This proof relates the security of BB84 protocol to an entanglement purification protocol [140] and quantum error correction codes [141]. It also means that the key generation rate, can be expressed in terms of the bit and phase errors which are decoupled from each-other,

$$r_{\text{BB84}} = 1 - H(Q_{\text{Z}}) - H(Q_{\text{X}}). \quad (5.1)$$

Here, $H(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ evaluates the binary entropy of x [142], and Q_{Z} and Q_{X} are the bit and phase errors respectively. If we consider the case where $Q_{\text{Z}} = Q_{\text{X}}$, then in order to have a non-zero key rate then Q_{Z} and Q_{X} must be below $\sim 11\%$.

5.1.2 Conference key agreement

Extending beyond the case where just two parties wish to establish a secure key, we lead the discussion onto how multiple users could establish a common unique key between themselves. In such a scenario, a group of users can exclusively establish a “conference” key to encrypt and decrypt subsequent messages. Conference key agreement, a generalisation of the key distribution task extended to the generation of an information-theoretic secure key between multiple users, can be executed in two distinct ways. The first way invokes 2-QKD primitives to generate keys in a pairwise process¹. Then, after this process has been iterated between pairs of users, a bitwise XOR operation transforms the pairwise keys into a unique common key.

The alternative method to obtain a conference key is to employ genuine multipartite entanglement (GME) in the form of a GHZ state. With a single resource state, the set of users can generate the unique common key directly. Recent proposals, one analogous to the six-state protocol [144] and the other analogous to BB84 [143] employ GME to generate a secure conference key. The latter of these was experimentally performed by M. Proietti *et al.* in Ref. [128]². A GHZ state shared by Alice to a number of Bobs, exhibits the desired criteria for a conference key protocol, as outcomes of measurement in the \mathbb{Z} basis are perfectly correlated, random and uniformly distributed. Conversely, if a Bell state establishing bi-partite correlations between Alice and Bob, then there for every local basis for Alice, there is a basis for Bob that is perfectly correlated, not good for establishing conference keys. In the conference key protocol, \mathbb{X} -measurements and some \mathbb{Z} -measurements are used to estimate the quantum bit error rate (QBER). In the \mathbb{Z} basis, the QBER $Q_{\mathbb{Z}}$ is the probability that at least one of the Bobs obtains an outcome that differs from Alice. More explicitly, the QBER $Q_{\mathbb{Z}}$ is defined as,

$$Q_{\mathbb{Z}} = 1 - \text{Tr}[\rho_{\text{GHZ}} (|0\rangle\langle 0|^{\otimes N} + |1\rangle\langle 1|^{\otimes N})], \quad (5.2)$$

$$= (1 - \langle \mathbb{Z}^A \mathbb{Z}^{B_i} \rangle) / 2, \quad (5.3)$$

for $i = 1, 2, \dots, N$. We know that the GHZ state only reveals perfect correlations

¹Neither the BB84, E91 or BBM92 can be generalised to multiple users, so one must deploy protocols outlined in Refs. [143, 144]

²A good resource for further, more advanced CKA analysis can be found in Ref. [145].

in the \mathbb{Z} basis so evaluating the phase error, $Q_{\mathbb{X}}$, requires one to calculate,

$$Q_{\mathbb{X}} = (1 - \langle \mathbb{X}^{\otimes N} \rangle) / 2. \quad (5.4)$$

If it is indeed a GHZ state that is shared between Alice and Bobs, then $Q_{\mathbb{Z}}$ and $Q_{\mathbb{X}}$ should evaluate to zero. Latter on in this chapter we exploit calculations of $Q_{\mathbb{Z}}$ and $Q_{\mathbb{X}}$ for the purpose of state verification.

To then perform the N-BB84 the following procedure is implemented.

- A quantum server prepares and distributes a maximally entangled GHZ state $|\text{GHZ}\rangle \equiv (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$ to N -users over L rounds and does not require to be trusted.
- There are two types of rounds. The first, type-1, consists of measurements in the \mathbb{Z} -basis. The second, type-2, occurs with a probability of p and consists of measurements in the \mathbb{X} basis. The total number of type-2 rounds is given by $m = L.p$.
- Users then need to verify the security of their key by performing parameter estimation. They announce their outcomes for a subset of type-1 rounds of size m , and all m type-2 rounds. This lets the users define the QBER for measurements in the \mathbb{X} and \mathbb{Z} bases. For a GHZ state, appropriate correlations means that the QBER in both cases should be zero.
- The remaining $n = L - 2m$ bits form a raw secret conference key, and classical post-processing can begin.

For assessing the upper bound performance of this protocol, we can operate in the limit of $L \rightarrow \infty$, letting us determine the asymptotic key rate (AKR) as a fraction of the secret bits. This upper bound results from the fact that in the finite key regime, bits are consumed for finite-key correction terms and additional security parameters, the derivation of the fractional key rate is present in Ref. [143].

5.1.2.1 Asymptotic key rate comparison

Comparing the AKR of N-party QKD method against a 2-party and one-time-pad (pairwise XOR) QKD method to establish a key between the same subset of users requires the calculation of the AKR in both cases. The AKR of the N-party QKD protocol, where the resource state is transformed into a GHZ state shared by Alice, Bob₁, Bob₂ and Bob₃, is given by [143]:

$$\text{AKR}_{\text{NQKD}} = 1 - H(Q_{\mathbb{X}}) - \max_{i \in \{1,2,3\}} H(Q_{AB_i}), \quad (5.5)$$

where again, $H(x)$ is the binary entropy, $Q_{\mathbb{X}}$ is the probability that the \mathbb{X} outcomes of the parties multiply to -1 (or 1 if ascribing logical outcomes):

$$Q_{\mathbb{X}} = \Pr(\mathbb{X}_A \mathbb{X}_{B_1} \mathbb{X}_{B_2} \mathbb{X}_{B_3} = -1)$$

and Q_{AB_i} is the QBER in the \mathbb{Z} basis between Alice and each Bob

$$Q_{AB_i} = \Pr(\mathbb{Z}_A \neq \mathbb{Z}_{B_i}).$$

For the 2-party QKD, Bell states—which are distilled from the resource state—are established between either a between Alice and Bob₃ (AB_3), Alice-Bob₁ (AB_1) and Bob₂-Bob₃ (B_2B_3). Suppose that the asymptotic (bipartite) key rates—secret bits per Bell state—of pairs of users denoted as AB_3 , AB_1 and B_2B_3 are obtained by performing the “traditional” BB84 calculation, as in Equation (5.1). This means that the secret key rate is given by:

$$r_{AB_3} = 1 - H(Q_{\mathbb{X}}^{AB_3}) - H(Q_{AB_3}) \quad (5.6)$$

$$r_{AB_1} = 1 - H(Q_{\mathbb{X}}^{AB_1}) - H(Q_{AB_1}) \quad (5.7)$$

$$r_{B_2B_3} = 1 - H(Q_{\mathbb{X}}^{B_2B_3}) - H(Q_{B_2B_3}), \quad (5.8)$$

where $Q_{\mathbb{X}}^{AB_3} = \Pr(\mathbb{X}_A \neq \mathbb{X}_{B_3})$.

Now, we want to establish an ℓ -bit conference key among Alice, Bob₁, Bob₂ and Bob₃. With a 2-QKD strategy, this is achieved by first establishing ℓ -bit pairwise keys between AB_3 , AB_1 and B_2B_3 and then using the established keys to transmit—via one-time-pad—the ℓ -bit conference key. Note that in order to establish an ℓ -bit

secret key between Alice and Bob₃, we need ℓ/r_{AB_3} Bell pairs between them, which amounts to the same quantity of resource states. Similarly, the other pairwise keys require ℓ/r_{AB_1} and $\ell/r_{B_2B_3}$ Bell pairs respectively. However, since in this case the resource state can yield two Bell pairs in one network use, the required number of resource states is $\max\{\ell/r_{AB_1}, \ell/r_{B_2B_3}\}$. This means that with a 2-QKD strategy we require two network usages compared to one for N-QKD, giving a key rate advantage of a factor of 2.

By summing the number of required resource states, the asymptotic conference key rate of 2-QKD reads:

$$\text{AKR}_{2\text{-QKD}} = \lim_{\ell \rightarrow \infty} \frac{\ell}{\frac{\ell}{r_{AB_3}} + \max\left\{\frac{\ell}{r_{AB_1}}, \frac{\ell}{r_{B_2B_3}}\right\}} \quad (5.9)$$

$$= \frac{1}{\frac{1}{r_{AB_3}} + \max\left\{\frac{1}{r_{AB_1}}, \frac{1}{r_{B_2B_3}}\right\}}. \quad (5.10)$$

Assuming that $r_{AB_3} = r_{AB_1} = r_{B_2B_3}$, we observe that the $\text{AKR}_{2\text{-QKD}}$ is at most 0.5, meaning that at least two network usages are required before a single conference key bit is obtained.³³

5.2 Experimental Network Communication

Before any experimental results, let us explicitly explore how a network resource state could be used to compare the performance of a 2-party protocol to a 4-party protocol.

Within the graph state framework (discussed in Chapter 1), are a set of tools which allow us to perform local, single-qubit operations onto our state, which can transform a starting state into a more desirable target state. Performing local complementation operations onto specific nodes of the starting graph, followed by measurements and local rotations, we can either distill a GHZ state between four users, or a Bell state pairwise between all combinations of the four users who share the four-qubit GHZ state. Our network resource state takes the form of the forks of a *trident*, so for the following parts of this thesis, we shall be referring to this target graph state as the trident graph. Performing local complementation onto this graph—by allocating specific target nodes—we can obtain different six-photon states with alternative graph structures. Whilst these states remain locally equiv-

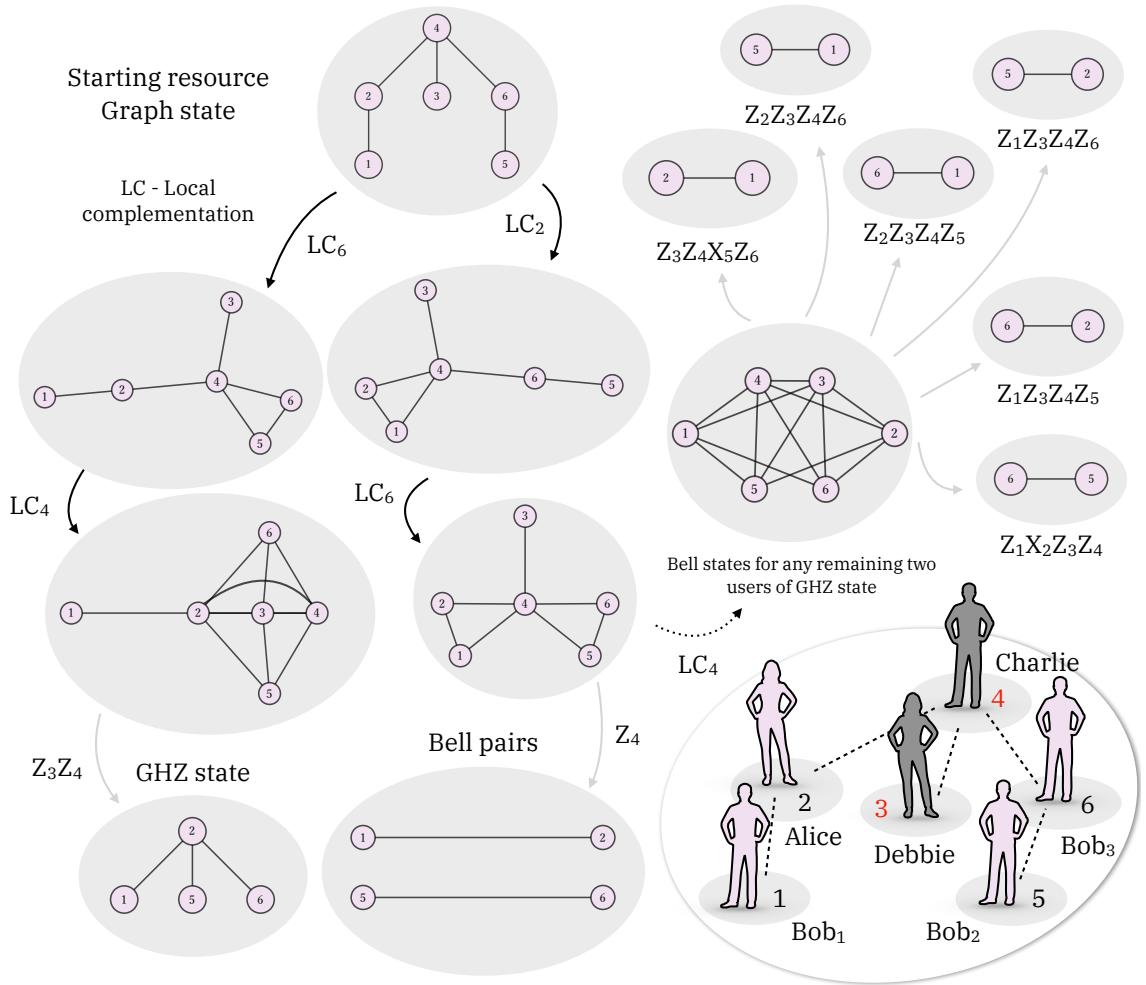


Figure 5.1: Summary of the graph state protocol. Starting with a graph state, one can perform local complementations in order to produce other graph states. A nice property of our starting graph, which is also displayed at the bottom right, is that if 6 users each possess a bi-partition of this state, then 4 of the 6 users can partake in an investigation as to the most efficient means for them to establish a conference key. The bottom right graph contains the 6 users and their respective names and indices. Users 3 (Debbie) and 4 (Charlie) act as network routers, and do not partake in the conference key agreement. Alice, Bob₁, Bob₂ and Bob₃ can establish pairwise correlations with each-other via a Bell state, or all share a GHZ state. In order to compute the conference key rates, the users who are not involved in the are required to make measurements on their partitions, else the protocol will fail.

alent, their structure is what provides a crucial role in being able to distill smaller scale states. There is no analytical method for identifying which graph structures are useful for a specific purpose, but possessing a computational tool box that allows one to implement experimentally accessible operations onto a graph theoretically, creates a playground to explore what you can and cannot do with specific graphs. This is ultimately how we arrived at a useful family of graphs, and an interesting “blueprint” outlining well defined steps that can be translated from theoretical model to experimental realisation.

The trident graph is locally equivalent to three specific graph states, then upon attaining these graphs with single-qubit unitaries, performing measurements in the Pauli basis on specific nodes, we can produce all the states we need in order to compare QKD methods. Figure (5.1) outlines the protocol we perform in this work and provides some important graphical context. Notably, is the way the trident graph forms the topology of a quantum network, containing six nodes, a subset of nodes constitute users who wish to communicate, these include Alice, Bob₁, Bob₂ and Bob₃, whilst the remaining two-users are so-called network users and are denoted as Charlie and Debbie. The aim for Charlie and Debbie in the protocols is to comply with the tasks the network demands, if they do not comply and perform measurements they should not, then they generate detectable errors.

Translating the graph notation into its circuit equivalent, helps provide a deeper understanding on the physical state. It also helps prepare blueprints for how the experiment is performed, this will be discussed in more detail in a subsequent section. Translating from the visual representation of a graph state to circuit notation is simple, but the translation from circuit notation to what we will call the optical circuit notation is not so simple. This is because the CZ gate, although experimentally accessible, is very lossy, with a probability of success at 1/9. Linear optical fusion gates have a much better probability of success of 1/2, so we found a means of obtaining the trident graph with fusion gates as opposed to CZ gates for experimental feasibility. In order to theoretically obtain the correct density operator for each six-qubit graph in Figure (5.1) we used IBM's quantum information toolbox Qiskit [58]³. Obtaining the density operators was not necessary for the experiment protocol, but was necessary for creating a simulation of the protocol.

5.2.1 Generating an Optical Graph State

In order to generate any optical graph state we need a few resources. Specifically, for the graph state we want to prepare, we require two pairs of singlet states, more precisely Bell states prepared as $|\Phi^+\rangle$, and a pair of separable photons prepared in the diagonal basis. Along with these resource states, we require fusion gates (type-II) to perform the non-local operations to access multi-partite entanglement. The final requisite are sets of local operations, which allow the optical generated state to

³Just a note to the reader that, if they do want to use Qiskit, then be careful defining your circuit as the indexing of the qubits are inverted.

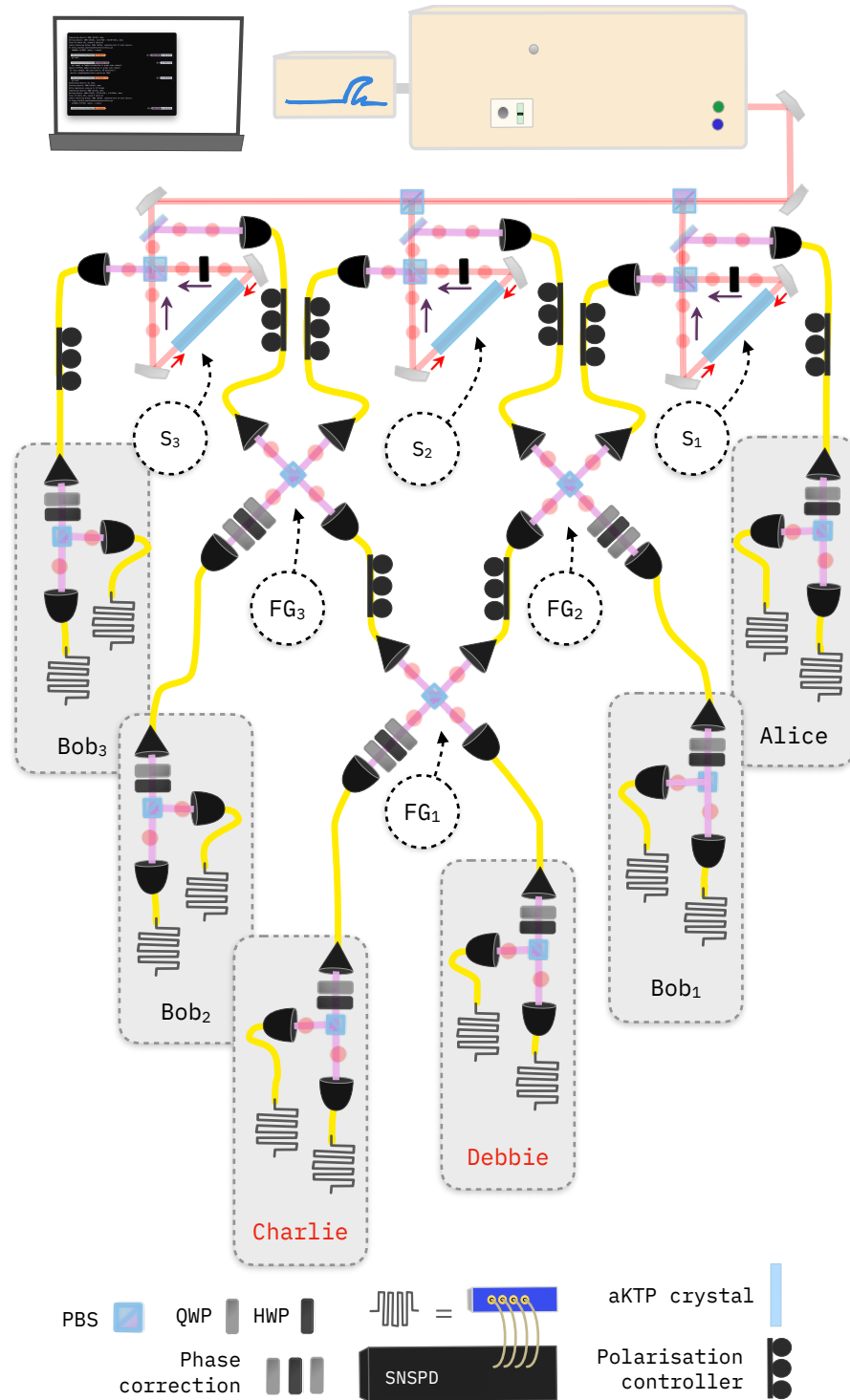


Figure 5.2: Experimental arrangement for generating 6 photon graph state. Schematic of linear optical components as well as PDC sources embedded inside sagnac interferometers. The result from this scheme, upon detection, is a 6 photon state that is locally equivalent to the Trident graph state. Three PDC sources, S_1, S_2 and S_3 —two of which are prepared as a maximally entangled state, $|\Phi\rangle^+$ —the other one of which is prepared as a separable source, preparing two photons aligned to $|D\rangle$. These states are inputs for three Type-II fusion gates, FG_1, FG_2 and FG_3 . Contained within these gates, are phase correction wave-plates. Once photons propagate through the optical circuit, they are detected by SNSPD's and the photon counts are processed by a logic box operating in logic mode to be able to handle the stream of counts arriving at the detectors, and to be able to process 6-fold arrivals quickly.

be rotated to the correct starting state, and projective measurements. Figure (5.2) depicts the optical arrangement for generating a six-photon state that is locally equivalent to a family of graph states that contains the trident and whose orbit we seek to explore. This equivalence comes from the fact that for an N-qubit stabilizer state, there is a set of local Clifford operations acting on each qubit of the state satisfying

$$|\psi\rangle = \bigotimes_{j=1}^n U_{C_j} |\mathbf{G}\rangle. \quad (5.11)$$

With reference to Figure (5.2), source 1 and 3 both generate $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{56}$ respectively, whilst source 2 generates a separable state $|\mathbf{DD}\rangle_{34}$. The optical circuit could be described as having a depth of two. The first level contains two Type-II fusion gates which each fuse together the separable state with a Bell state. These fusions act on modes 2, 3 and modes 4, 5. The next layer of the optical circuit contains one more fusion gate which fuses modes 3, 4 and produces the following state:

$$\begin{aligned} |\Psi\rangle_{\text{initial}} = \frac{1}{\sqrt{8}} (&|\mathbf{HHHHHH}\rangle - |\mathbf{HHHHVV}\rangle - |\mathbf{HHVVHH}\rangle - |\mathbf{HHVVVV}\rangle \\ &- |\mathbf{VVHHHH}\rangle + |\mathbf{VVHHVV}\rangle - |\mathbf{VVVVHH}\rangle - |\mathbf{VVVVVV}\rangle) \end{aligned} \quad (5.12)$$

Note however, that this is not the desired target state (the trident), but something locally equivalent to the desired state satisfying Equation (5.11).

5.2.2 Transforming into an Optical Graph State

In order to determine how to rotate the optically generated state, $|\Psi_{\text{initial}}\rangle$, into the desired trident graph state, $|\Psi_{\text{target}}\rangle$, we can use a rather inelegant approach that searches all possible combinations of local unitary operations applied to each qubit. This search spans 15,625 different transformations applied to the optical state. Computing the fidelity between the optically rotated state and the target graph reveals that the following transformation obtains the result we require:

$$(\mathbf{H} \otimes \mathbf{Z} \otimes \mathbf{H} \otimes \mathbf{Z} \otimes \mathbf{H} \otimes \mathbf{Z}). |\Psi\rangle_{\text{initial}} = |\mathbf{G}\rangle_{\text{target}}. \quad (5.13)$$

Figure (5.3) shows the computed fidelity along with the index of the transformation applied to the initial state. It reveals that out of the 15,625 transformations only 1

rotates the initial state into the target state.

Now that we have obtained the target graph state, we need to check that the LC operations we want to perform coincide with obtaining the desired graph states in the next steps towards distilling the different resource states. Given that we have the density operator for all the graph states we need to obtain, this check is just a matter of applying the correct local rotations to the initial state and again, verifying we arrive at the correct state by computing the fidelity. Figure (5.4) shows a matrix plot of the density operators for the initial state, the required rotation and the desired state, forming an example of how we simulate the protocol to evaluate whether the transformations we will apply to the experimental state are correct.

5.2.2.1 Distilling states

We now face the problem that transforming graphs, or more generally stabilizer states, into tensor products of bipartite Bell pairs, or just a set of Bell pairs between specific vertices (or users in our network) using only a certain class of local operations and classical communication is a NP-complete problem [146]. As previously mentioned however, we have found via playing with a graph toolbox starting with the trident graph, we can perform transformations in order to distill a set of Bell pairs on specific vertices using only single-qubit (local) Clifford operations, single-qubit Pauli measurements and classical communication (LC+LPM+CC). Likewise for GHZ state distillation from arbitrary graphs, if we wish to arrive at a GHZ state between a specific set of vertices [147] or if we require a GHZ state of fixed size [147], the task is NP-complete. This means that as a network primitive, knowledge of the initial shared graph structure as well as the structure of the distilled states are an

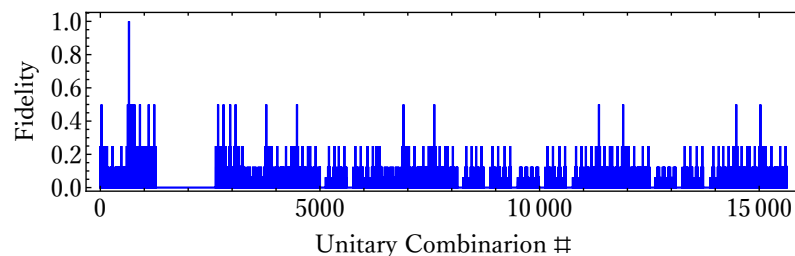


Figure 5.3: Transformation search to find correct combination of local unitary transforms on each qubit to rotate the experimentally generated state into the desired target Graph state. The search consists of computing the fidelity of the target state, with the initial state rotated by a combination of single-qubit unitary operations.

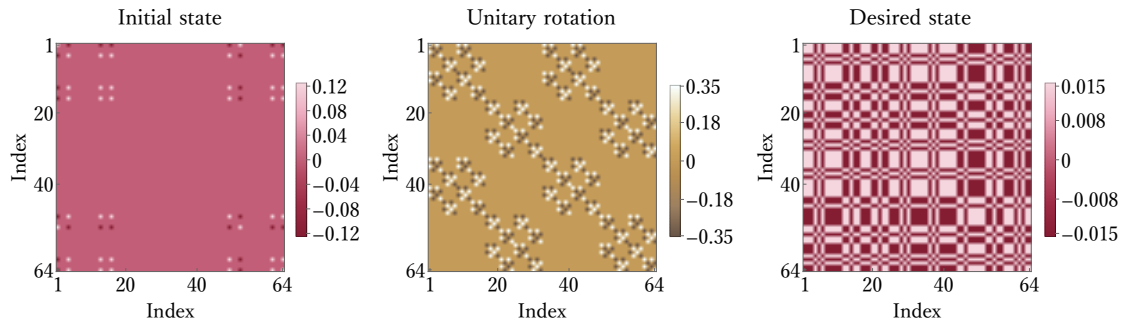


Figure 5.4: Matrix plots of the initial state, desired state and the unitary operation to transform between them. In order to confirm that we can obtain all the desired graph states, we need a simulation containing all of the steps of the protocol. This means that every transformation needs to be correctly defined and all operations, and states defined with the density operator formalism. As an example we show the initial, experimentally prepared state, the rotation applied to the initial state which is composed of the Kronecker product of Hadamard and \mathbb{Z} single-qubit operations and the desired trident graph state.

essential resource. Although deriving these distillation steps is inefficient, there is no reason why a repository of network compatible graphs as well as LC+LPM that enable the distribution of either GHZ states or Bell states to a sub-group of users cannot be built.

We will now outline the steps to attain the required states from the network resource (trident graph). To arrive at a four-user GHZ state, the initial trident

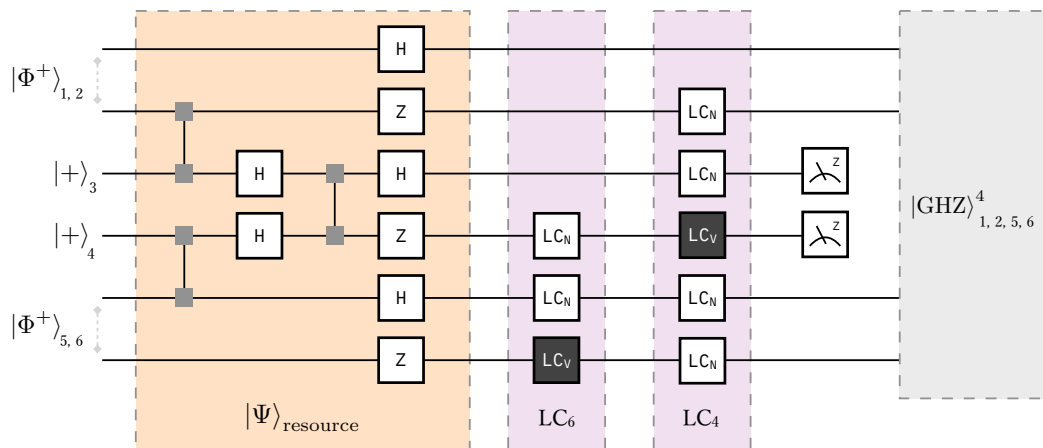


Figure 5.5: Blueprint for generating GHZ state. For obtaining a GHZ state between qubits 1, 2, 5 and 6 the initial resource state (the area of the circuit highlighted orange), requires two local complementation operations (the area of the circuit highlighted purple). The local complementations performs local rotations onto the target vertex and its neighbours. Finally, Pauli measurements performed on qubits 3 and 4 leave the remaining qubits in a 4-qubit graph state locally equivalent to a GHZ state up to Hadamard rotations on qubits 1, 5 and 6.

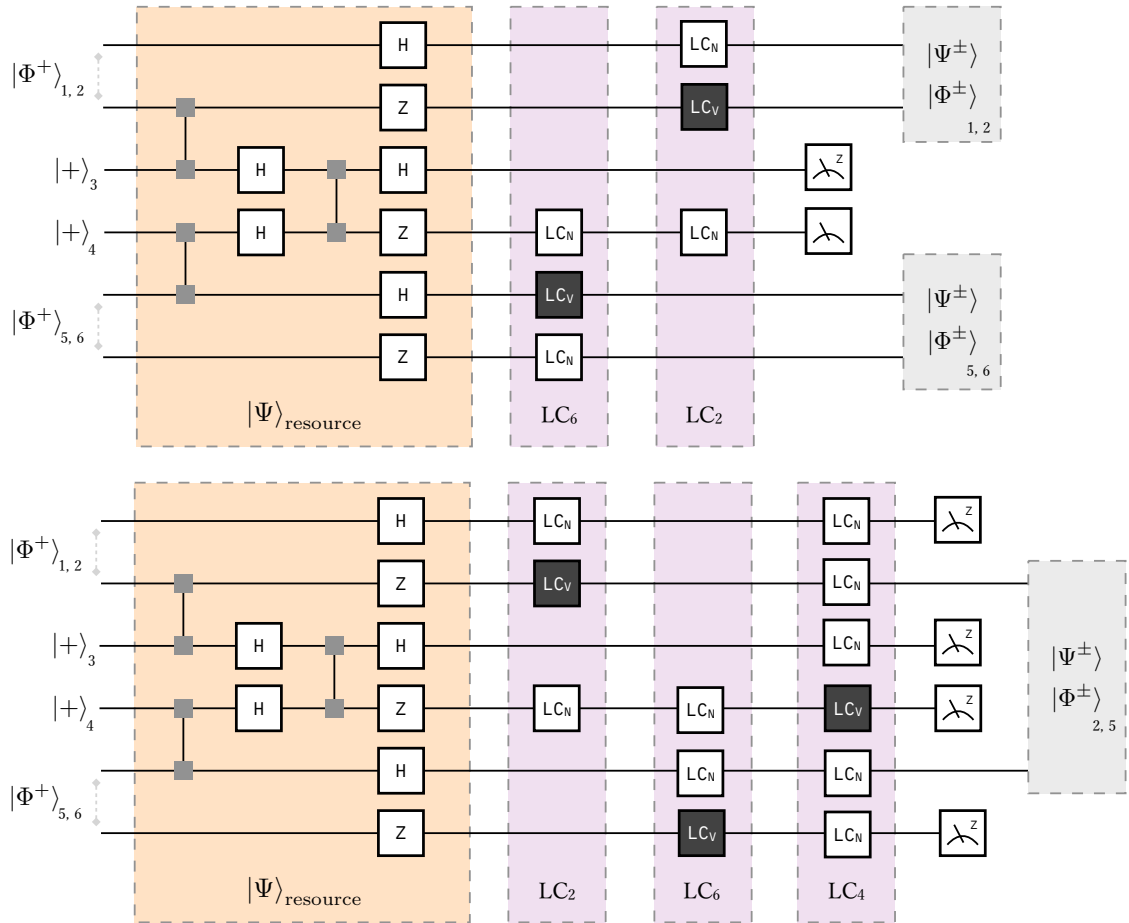


Figure 5.6: Blueprint for generating Bell states. There are two network usages required to distill three Bell states between the same subset of users who share a GHZ state (users 1, 2, 5 and 6). Each usage is outlined in this figure, the top distilling two Bell states, the bottom distilling only one. But this single Bell states allows the 4 users to obtain a conference key. The resource state preparation is highlighted in orange, whilst the required operations in purple. Much like in the case of the GHZ state, the states distilled are actually locally equivalent to Bell states under Hadamard rotations on a single bi-partition.

graph has to undergo two local complementation operations applied to vertices 6 LC_6 and 4 LC_6 . These local rotations are followed by projections in the Z basis on qubits 3 and 4, leaving the remaining qubits in a state locally equivalent to a GHZ state. This local equivalence stems from the fact that, although taking the graphical form of a GHZ state, Hadamard rotations are required on the leaf nodes of the graph corresponding to qubits 1, 5 and 6. Figure (5.5) depicts a pseudo quantum circuit describing the exact actions on each qubit, omitting the final Hadamard rotations. The origin of these rotations come from the fact that qubits in the graph formalism are initialised in the state $|+\rangle$.

To attain Bell states between different subsets of users, we must first acknowledge

that this subset of users must be the same subset sharing the GHZ state. This means that a combination of the users—or equivalently vertices—or correspondingly qubits—1, 2, 5 and 6 must be able to share a Bell state, a requirement of being able to implement two-party QKD. There are several ways of deriving Bell states that fully span this subset. But to perform conference key agreement with two-party QKD we need two distinct network usages. Each of these usages then allows a subset of users to perform two-party QKD. For example, we choose to initially distill two Bell states between users 1, 2 and 5, 6, designating the first network usage. An extra network usage is then required to obtain another Bell state, this time each partition of this state must be shared between either 1 and 5 or 1 and 6 or 2 and 5 or finally 2 and 6. We chose to obtain a Bell state between users 2 and 5 in this second network usage. The first and second network usage each require different local complementation operations but crucially still share the same resource state. A full outline of containing the operations for each network usage is outlined in Figure (5.6). Something to note about the distillation of the two Bell states in the first network usage is that, from inspection of the graphical representation of the trident, simply a Z measurement on qubit 3 creates identical Bell states to the first network usage. This is possible if, and only if, the graph was generated deterministically. Using probabilistic sources and non-deterministic fusion gates means we need to and post-select on six-fold coincidences, ruling this approach out for our architecture.

5.2.3 Experimental Preparation of State

Now, let us discuss how we prepare the optical state, locally equivalent to the trident. A Ti:Sapphire laser which, as already mentioned, possesses a non-ideal sech^2 -shaped spectral envelope, pumps our crystal with a central wavelength of 774.9nm and a pump pulse duration of 1.3ps which is optimal for our domain-engineered crystals. Each source, a sagnac interferometer containing one of our domain-engineered crystals, produces degenerate photons by being kept at a constant specific temperature via an oven controlled by a PID unit. Initially aligned and configured to generate an larger photonic cluster state, the pump was focussed into the crystals with a 40cm lens in order to increase the effective squeezing to attain high photon pair production rates, and collection distances were chosen to further maximise the brightness at the

expense of heralding efficiency. Unfortunately, this condition was not ideal for this experiment. We have already made plans to instead maximise heralding efficiencies by increasing the spot size in the crystal, effectively reducing the squeezing, increasing the heralding. More details on this point will be provided in the discussion, conclusion and later on in this section where we discuss the overall performance of this experiment.

First step to prepare the six-photon state was a tomography of the Bell states $|\Phi^+\rangle_{1,2}$ and $|\Phi^+\rangle_{5,6}$ with a reference set-up that would stay consistent. The reason for this is that verifying the Bell states inside the circuit may not be able to reveal any fundamental issues with the sources themselves. Then, after attaining sufficient state fidelities and purities, these singlet states were plugged into the optical circuit described earlier. Due to the nature of the circuit and the polarisation optics in the spatial modes of the outputs of $|\Phi^+\rangle_{1,2}$ and $|\Phi^+\rangle_{5,6}$, we can map the correct populations to the arrival of photons in specific sets of detectors. This is a required step, as in-between verifying the Bell states in the reference set-up and plugging them into the optical circuit, the different optical fibres impose arbitrary polarisation rotations to each qubit which needs to be corrected against. The Bell states are re-prepared, ensuring that we can achieve the same contrast in populations we saw when we independently prepared the states with the reference set-up (containing optics to perform projection measurements on each qubit of the state). Performing the appropriate single qubit rotations in order to correct for rotations the new fibres have imposed was carried out with sets of polarisation controllers, which can perform rotations spanning the full Bloch sphere. Repeated for both the Bell states, we look at the detection outcomes owing to where the photons have travelled in the circuit and prepare each of the states again, initially in the computational basis. Any phase that was picked up in the diagonal basis, equivalent to distinguishing between preparing $|\Phi^+\rangle$ and $|\Phi^-\rangle$, is corrected for in the phase correction components which perform rotations in the $\mathbb{X} - \mathbb{Z}$ plane to one of the output qubits after each fusion gate, but this will be addressed later. The separable state is prepared in a similar manner (by looking at the counts in a set of specific detectors), but a linear plate polariser ensures that the photons are prepared as $|D\rangle$ meaning the preparation is a lot easier.

Now that the states are prepared correctly, we need to be able to check whether the fusion gates are configured correctly aswell. A subset of detection channels can

be used for the verification of each fusion gate. We validate the performance of the fusion gates by conducting a short independent two-photon interference measurement, measuring the visibility by adjusting the temporal delay and recording a HOM dip adhering to the discussion in Chapter 4, Subsection (4.2.4). Verification of the fusion gates occurs throughout the experimental investigation and each of the three fusion gates were certified as operating sufficiently when interference visibilities of $> 90\%$ were achieved at a pump power of 100mW. The phase components we need to correct, emanating from the preparation of the state and the PBS in the fusion gate, are corrected for by a manual phase correction arrangement in one output of the fusion gate. This arrangement consists of two QWPs with a HWP sandwiched in between.

After our first few attempts at preparing the correct state, we added another means to verify that we are on the correct path to preparation. The first two fusion gates in the circuit interfere a photon from a bi-partition of a maximally entangled state and a photon prepared in the state $|D\rangle$. Succeeding the fusion gate, we have effectively produced a GHZ state. More explicitly, consider $|\Phi^+\rangle_{1,2}$ and $|D\rangle_3$. These state interfere on a PBS due to the operation of a type-II fusion gate, and the output from a simple calculation is a GHZ state. The same can be said for $|\Phi^+\rangle_{5,6}$ and $|D\rangle_4$. By measuring the populations of these “intermediate” GHZ states in the \mathbb{Z} basis, again by tracing their populations through the optical circuit, we can determine if the fusion gates are operating correctly. Measuring the populations of these GHZ states in the \mathbb{X} basis, represents another metric beyond polarisation HOM interference scans to ensure the phase correction is being applied correctly. Once fusion gates 2 and 3 are verified, we can finalise the state preparation by ensuring that fusion 1—and its phase compensation—has also been configured correctly. This is much easier than the other two fusion gates, as it can be verified with dependent photon interference. By this I mean we only need to interfere two photons from the same source but otherwise following the normal procedures for optimising a fusion gate, like what was discussed above. This concludes any tweaks we make to the optics controlling the state production and the subsequent propagation through the circuit, so we choose to measure a a set of observables of the six-photon state. This forms a quick sanity check confirming that so far the state preparation has been successful. The observables we allocated to this check were: $\langle ZZZZZZ \rangle$, $\langle ZZZZXX \rangle$, $\langle ZZXXZZ \rangle$ and $\langle XXZZZZ \rangle$. Figure (5.7) shows an example of the

measurement outcomes for one of these observables. Although indicative of having prepared the correct state, the success of these measurements does not tell us that we have prepared ρ_{initial} . Further details on this check as well as other verification techniques signifying the correct preparation of the state is a topic for the next section.

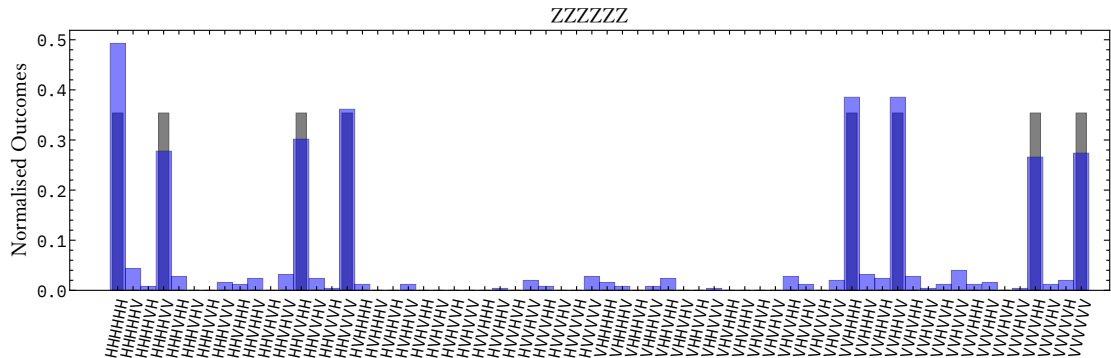


Figure 5.7: An example of one of the observables used to verify if we are preparing ρ_{initial} correctly. There are 64 possible outcomes for the results attaining to a measurement of the observable $\langle ZZZZZZ \rangle$. The grey bars correspond to the expected, theoretical populations of ρ_{initial} and the blue, slightly transparent bars represent the normalised experimentally measured populations.

5.2.4 Experimental verification of state

There are some important aspects that we will point out first that will hopefully aid the reader into understanding why we made certain choices in the verification of the state. Firstly, the six-photon count rate is low, with approximately 1 photon arriving every 10 seconds. Secondly, a full state reconstruction requires $3^6 = 729$ measurements, with each measurement having 64 outcomes. Finally, signals from the SNSPDs are processed by counting logic informing us of the projection measurement outcomes.

Let's start with the last point first, the counting logic needs to be able to handle vast streams of photons. As an example, in a 5 minute measurement of one of the populations of the 6 photon state there are 1.25×10^9 singles across 12 detectors, there are 225×10^6 two-fold coincidences across pairwise combinations of the 12 detectors and there are 66 six-folds belonging to all possible configurations of 6 from 12 detectors. The logic box, whose duty is to reconcile detection events to n-fold coincidences, has two operational modes: time-tagging and logic. In some preliminary testing, time-tagging mode would take a significant amount of time to

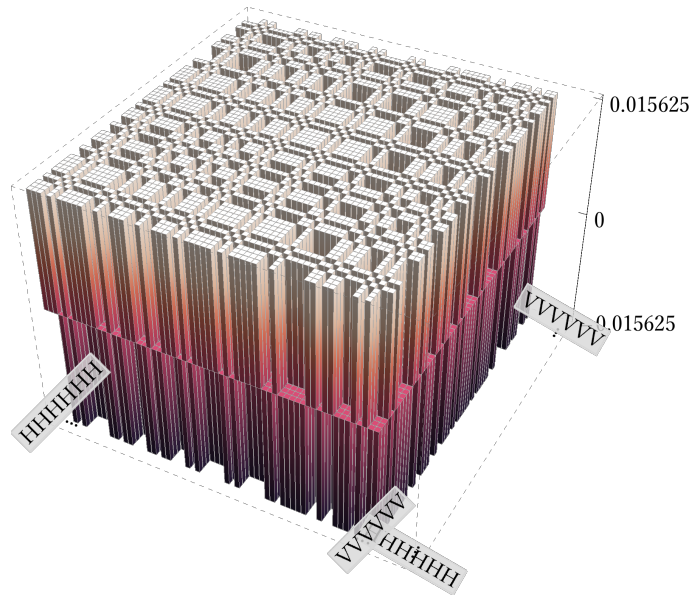


Figure 5.8: Density operator form of the Trident graph state. The Trident graph state density operator and the respective populations of the state indexed from HHHHHH through to VVVVVV. The lack of sparsity means that there is very limited contrast between the populations of projections. For a low six-photon generation rate with a Poissonian noise model and with a state with many non-zero elements in their density matrix the signal to noise ratio for each population is lower than a state whose density operator is sparse.

process detection events, such that for a 10 second measurement, the total time spent measuring would amount to 14 seconds. The scaling between the desired measurement time against the time spent measuring was non-linear with respect to the number of incident photons on the detectors, owing to the fact there are significantly more photons that are required to be stored in a buffer before being processed. Given the vast amount of detection events we need to handle, we would have to operate the time-tagging mode in very small increments of time to minimise the scaling between desired measurement time and time spent measuring. On the other hand, operating in logic mode—which does not require a buffer of stored tags—and allocating a measurement time of 10 seconds, the time spent measuring amounts to 10.1 seconds. Using logic mode, the time taken measuring is free from any unfavourable scaling with respect to the amount of incident photons, thus we chose to operate in this mode⁴.

Now, going back to the other important aspects we needed to consider; a com-

⁴Operating in logic mode was not as easy as just switching between modes. Unfortunately, the way temporal windows are configured on the FPGA meant that the assigned window is concatenated across all 12 channels. So a window of 1ns would actually span 12ns, meaning that our initial results whilst using logic mode contained uncorrelated photons from the pulses preceding and succeeding the targeted pulse. This resulted in unwanted populations in undesired bases and caused a lot of head scratching for a long time.

bination of the first and second point requires deliberation beyond just choosing an alternative means to verify the state. To begin with, full quantum state tomography is typically carried out with a number of measurements that form an over complete measurement set. Possessing the full reconstructed experimental density operator is useful for further analysis and modelling, it is was not necessary. In a tomography, after measuring mutually unbiased bases, the maximum likelihood algorithm reconstructs the density operator of the measured state [148, 149]. Collecting more statistics (sampling for longer or increasing the effective squeezing) during measurements will reduce errors in the outcome of the maximum likelihood algorithm by increasing the signal-to-noise (SNR) ratio, on account of the Poissonian photon statistics causing mixture in the final state. Let’s just delve into this point a little more; consider a single qubit prepared in $|H\rangle$, one would expect, when measuring in the X basis, to have a perfect distribution of counts, 50% in each measurement outcome. But Poissonian statistics tells us that, if for example we initially have 20 $|H\rangle$ photons, then measuring in the X basis we should expect $10 \pm \sqrt{10}$ and $10 \pm \sqrt{10}$ photons in each output. This means that we could have the situation where there are 13 photons and 7 photons measured in the eigenstates of the X basis. Clearly, running the tomography and the maximum likelihood algorithm would not reveal that the photons were prepared in $|H\rangle$. Only counting longer, increasing the SNR, will improve the accuracy of the maximum likelihood algorithm in this context. Low photon rates concatenated with a huge number of measurements means performing a full tomography would require an amount of time experimental labs typically cannot afford.

In the end, for attaining some knowledge of the state we prepared, we decided to randomly sample a subset of measurements to perform a “partial” quantum state tomography. Only selecting measurements which would contain counts in a small number of bases meant we could run these measurements for longer, increasing read times and increasing the SNR. The reason we decided to run this measurement, was not only could it reveal errors in the state preparation that we missed, it can also highlight any non-local operations that are affecting state quality, by providing us with an estimate of the density operator describing, and purity of the state prepared. Subsequently, this partial tomography revealed some crucial insight into our measuring optics. Two sets of QWPs in our measurement stages had been mounted such that they were aligned to their slow axis whenever they should have

been aligned to their fast axis. Finding out which measurement states were effected and how we corrected them will be discussed in the section following this.

Back to our discussion on state verification, interestingly, there are methods for validating the state similar to entanglement witnesses. These witnessing methods require measurements of the stabilizers of the state. From Section 6.6.4 of Ref. [150], the authors state that a generalisation of entanglement witnesses and the detection of multi-partite entanglement is closely related to measuring how close an experimental state is to a given multi-partite quantum state. Demonstrations of such fidelity estimating protocols are present in literature [111, 151–155]. Although only requiring at most 2^N measurements, N being the number of qubits—ideal when we are operating with low rates—this technique only lower bounds the fidelity of the state. This is nothing more than bounding the proximity of your state, to the target target state, revealing nothing about the states density operator. Another means of state verification is to apply compressed sensing, which provides a technique for recovering a sparse vector from a small number of measurements [156, 157]. This method can reconstruct an unknown density matrix of dimension d and rank r with $O(rd\log^2 d)$ measurement settings [158], amounting to ~ 209 measurements for the experimentally generated state we desired in this work.

As we stated in the previous section, we allocated a set of observables to act as a quick check to determine if we have the state prepared correctly with the populations in the bases we expect them to be in. Importantly, something we have not explicitly mentioned yet is that we measure the observables of ρ_{initial} and not ρ_{trident} . The sparsity of the density operator for the experimental state (ρ_{initial}) means that identifying any counts populating bases where there should be no counts is easier and (as we explained already) when a limited number of photons are detected the SNR is favourable for states with less populated bases. Figure (5.8) depicts the density operator of the trident graph and shows just how many of the elements of the density matrix are populated.

5.2.4.1 Flipped wave-plates

Other than the slightly tedious method of correctly analysing every single wave-plate in the set up (and of-course being more careful in setting all the wave-plates up), we can use the subset of the tomographic measurement set we described in the previous

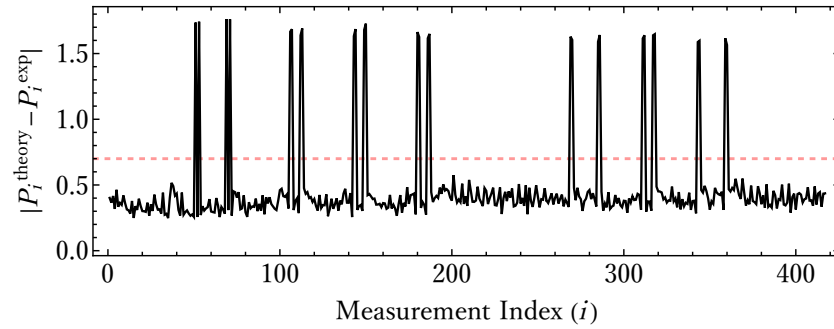


Figure 5.9: Finding the projections that contain incorrect measurement outcomes. Local rotations are trace preserving and only non-local interactions causing reduced purities, a consequence of miss-labelled measurement settings. Out of 417 observables, our partial state tomography revealed that 28 contained errors. These were determined by calculating the absolute of the difference between the theoretical populations in each basis of a given projector, and the correctly normalised experimental results for that projector.s

section, to verify if we do in fact have any wave-plates assigned to their slow axis rather than their fast axis. Flipped wave-plate settings will perform an incorrect measurement with respect to the measurement that is assigned to them. This applies a non-local, non-trace preserving operation onto the state, degrading the state purity. First step to fix any unwanted flips, is to determine which observables if any had populations in incorrect bases. By calculating the absolute of the difference between the theoretical populations in each basis of a given projector, and the correctly normalised experimental results for that projector, we can determine which (and how many) observables produced incorrect results. Figure (5.9) reveals that 28 out of the 417 observables contains an error. Conscious that when characterising QWPs, it is much easier to incorrectly assign their fast and slow axes, we ran a simulation that relabelled the measurement settings associated to measurement requiring the QWP to be rotated to its fast axis or to its slow axis in the sets of measurements forming our initial partial tomography. Only swapping projections in the \mathbb{X} and \mathbb{Y} basis, the simulation would flip the assigned measurement setting for an index assigned to each qubit. The results from this simulation inform us for which qubits the measurement settings require a re-labelling and the number of observables that contained errors. This subsequently revealed that QWPs in the measurement stages for qubit 5 and 6 were orientated to their slow-axis when they should have been at their fast axis. To fix this we re-mapped measurement settings for qubits 5 and 6 accordingly.

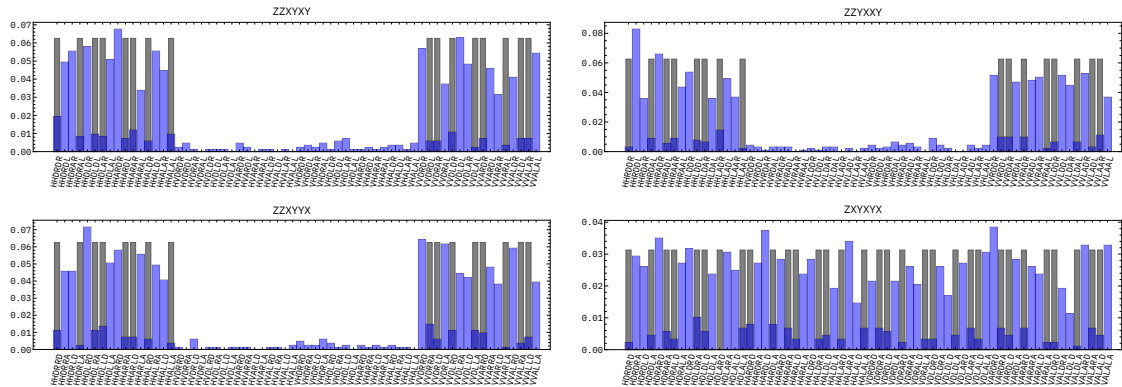


Figure 5.10: An example 4 of the 28 observables that contained errors. When analysing the partial quantum state tomography, we identified immediately that there was a re-labelling required for measurement settings. Inspection of the observables that contained the flip revealed that errors would occur only when projections were not made in the computational basis, owing to incorrectly assigned fast and slow axes of QWPs.

5.2.5 Obtaining desired state

After identifying which wave-plates were incorrectly set, we can apply corrections to these plates and re-run our partial tomographic reconstruction. Figure (5.11) shows the real and imaginary components of the reconstructed density operator. This operator was defined from a partial set of measurements and thus only produces an estimate of the state purity and fidelity were 56.5% and 65.6% respectively. Without a mathematical proof that would inform us otherwise, the reconstructed state is not fully faithful and cannot be used as a means of instructing us that we absolutely have the correct state. What we do know, can model and mathematically simulate, is that upon sets of well defined single-qubit operations applied to the initial state, we obtain Bell states and GHZ states. We also know, that evaluating Equation (5.5) for a GHZ state or Equation (5.10) for a Bell state and obtaining a non-zero values, confirms that we have established correlations indicative of having established a Bell state or GHZ state, which are only derived if we had the correct initial state $|\Psi\rangle_{\text{initial}}$. Finding correct sets of well defined single-qubit operations applied to the initial state distilling Bell state and GHZ states to calculate Q_Z and Q_X is therefore imperative for the communication protocol to work.

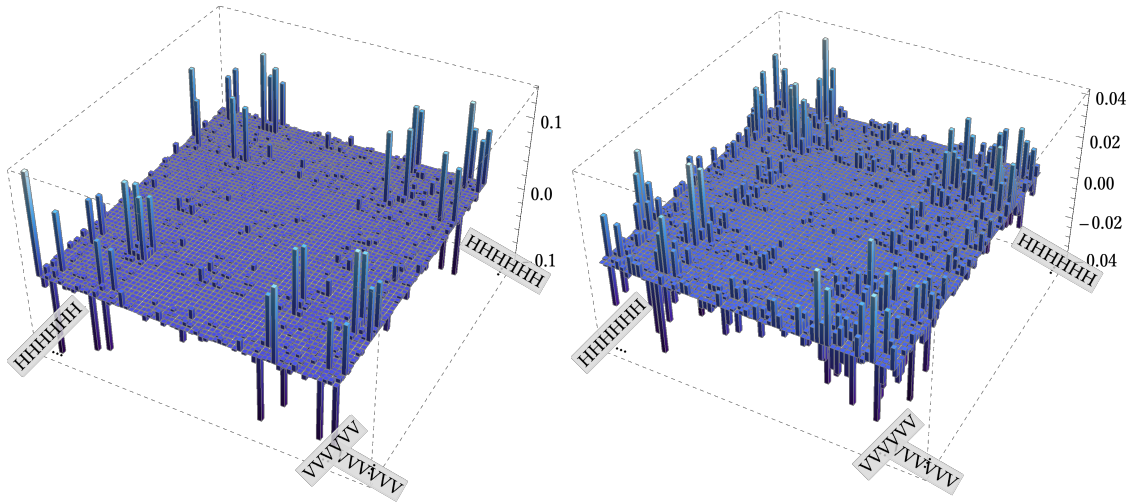


Figure 5.11: Reconstructed density operator from a partial quantum state tomography. A partial tomography let us reconstruct the real and imaginary parts of the density operator of our state. Although just an estimation and not the true density operator for the state we prepared, it serves as a useful tool for any simulations we wish to run. It was obtained in the same means one would reconstruct from a full over-complete measurement set of MUBs.

5.2.5.1 LC operations

Before being able to evaluate $Q_{\mathbb{Z}}$ and $Q_{\mathbb{X}}$, we need to perform the correct single-qubit operations on each qubit following the “recipes” outlined in Section 5.2.2.1 and shown in Figures (5.5) and (5.6). To do this, we encode the set of local operations applied to each qubit onto the measurement settings for the corresponding qubit. There are only two measurement settings for each qubit and these settings should be equivalent to projections in the \mathbb{Z} basis and projections in the \mathbb{X} basis. I think this is best understood if we run through an example. Say we want to measure the observables $\langle \mathbb{Z}_1 \mathbb{Z}_2 \mathbb{Z}_5 \mathbb{Z}_6 \rangle$ and $\langle \mathbb{X}_1 \mathbb{X}_2 \mathbb{X}_5 \mathbb{X}_6 \rangle$ of the GHZ state—which is in a four-photon sub-space of the initial state—giving us the information we need from the GHZ state to let us compute $Q_{\mathbb{Z}}$ and $Q_{\mathbb{X}}$. All other measurements are analogous to the example being outlined, but will require different sets of single-qubit unitaries to be encoded onto the measurement settings. Firstly, within the six-photon state space we have a graph. In order to obtain a GHZ in the four-photon state space, shared between Alice and the Bobs, Charlie and Debbie must make projections in the \mathbb{Z} basis on their bi-partitions of the state. But the operations they need to encode on their qubits means that their measurements are actually in the \mathbb{X} basis. So after appropriate encoding, to measure the observable $\langle \mathbb{Z}_1 \mathbb{Z}_2 \mathbb{Z}_5 \mathbb{Z}_6 \rangle$ of the GHZ state occupying the 4-photon state space, all users must measure the ob-

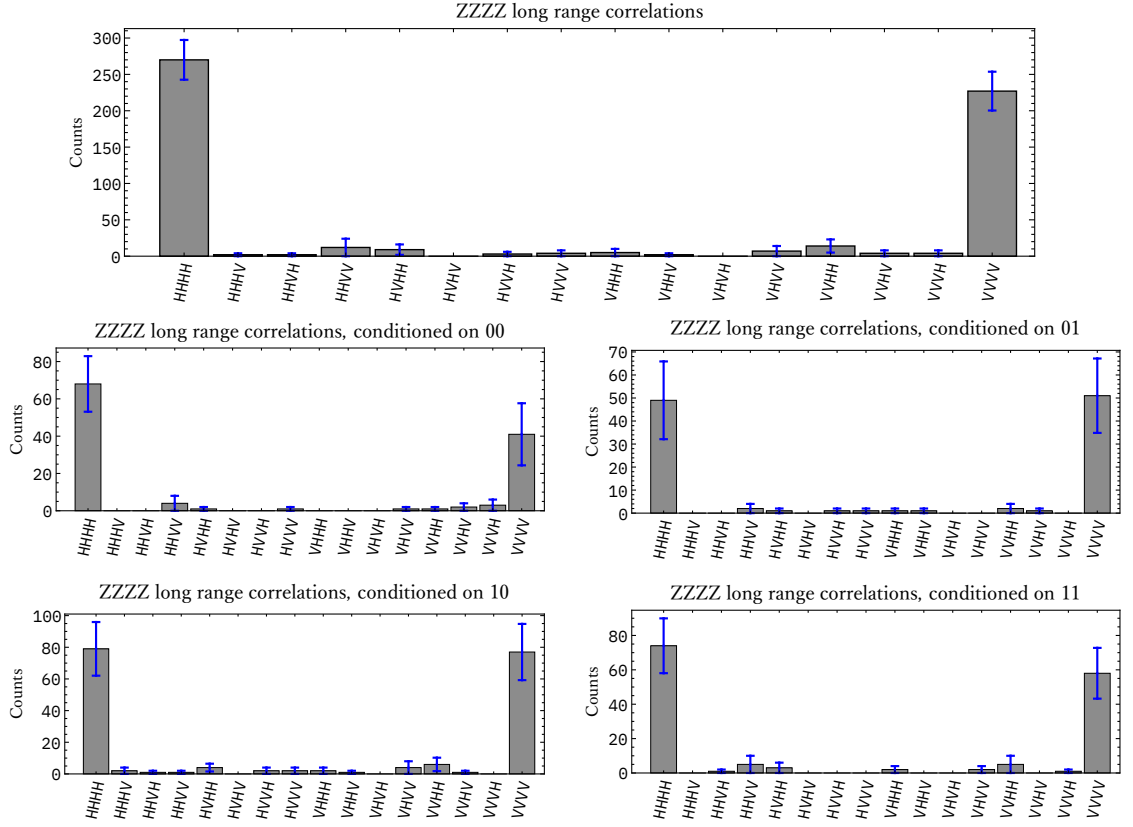


Figure 5.12: Establishing correct correlations in the \mathbb{Z} basis from a 4-photon GHZ state distilled from a 6-photon graph resource state. Encoding single-qubit operations onto measurement settings lets us measure the distilled GHZ state in the computational basis, verifying that we can establish the characteristic correlations and allowing us to evaluate $Q_{\mathbb{Z}}$ for parameter estimation. To establish a GHZ state between qubits 1,2, 5 and 6 (Alice and Bobs), users 3 and 4 (Charlie and Debbie) are required to announce their measurement outcomes so GHZ users know where to apply bit-flips in order for the users to reconcile their results attain the correct correlations (top plot). After performing the flips, long range correlations should be consistent and irrespective of whether Charlie and Debbie attained outcomes 00, 01, 10, or 11 (bottom four plots).

servable $\langle Z_1 Z_2 X_3 X_4 Z_5 Z_6 \rangle$. To measure the observable $\langle X_1 X_2 X_5 X_6 \rangle$ of the GHZ state occupying a four-photon state space, all network users must measure the observable $\langle X_1 Y_2 X_3 X_4 X_5 Y_6 \rangle$ correspondingly. Resulting from the effective network topology, each user holds a partition of the graph state and, as a consequence of the GME, whenever Charlie and Debbie perform a measurement they need to disentangle themselves from the system coherently. When Charlie and Debbie measure in the \mathbb{X} basis, they can attain either a 0 or a 1 (results in the computational basis). Any resulting GHZ will contain a phase rotation, conditioned on Charlie and Debbie's measurement results. This must be corrected for. Teleportation protocols require similar steps and the corrections are made in a feed-forwarding step [11], but in our case we apply all feed-forwarding as a post-processing step.

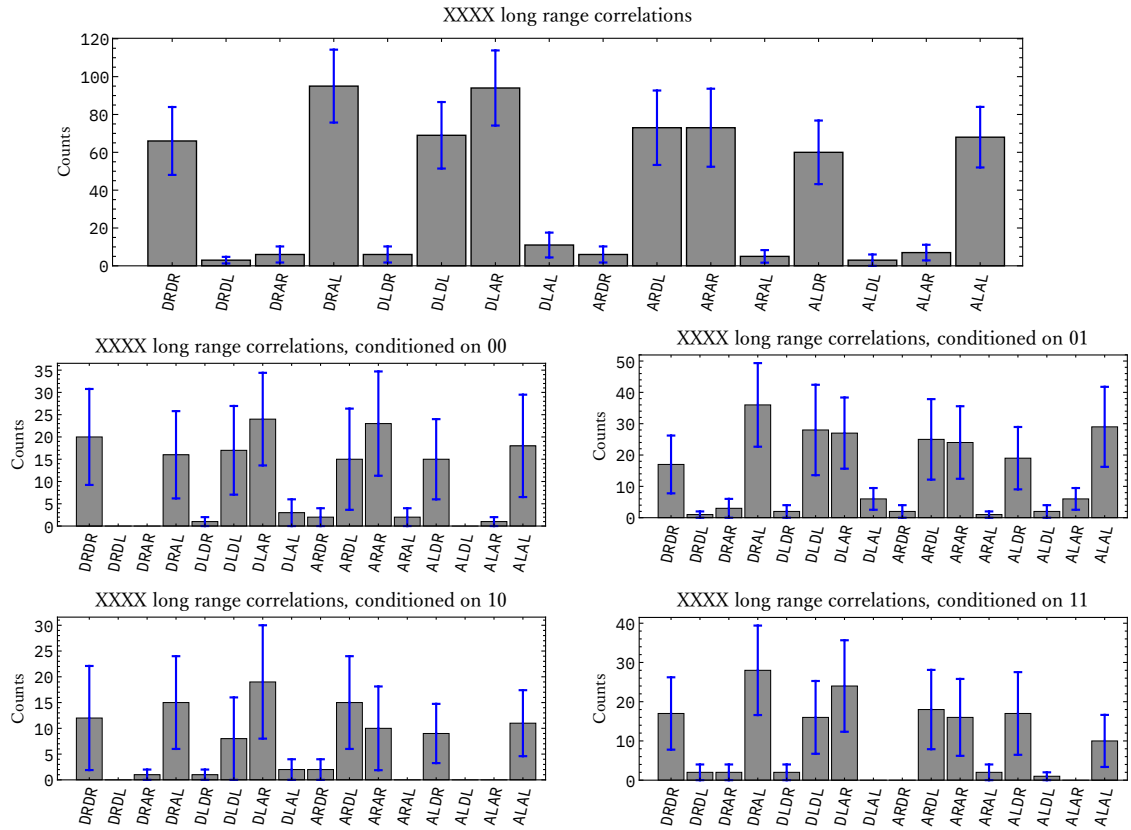


Figure 5.13: Establishing correct correlations in the \mathbb{X} basis from a 4-photon GHZ state distilled from a 6-photon graph resource state.. Encoding single-qubit operations onto measurement settings lets us measure the distilled GHZ state in the \mathbb{X} basis, verifying that we can establish the characteristic correlations and allowing us to evaluate $Q_{\mathbb{X}}$ for parameter estimation. Like for the \mathbb{Z} basis measurements, there is a bit-flip criteria conditioned on the measurement results attained by Charlie and Debbie. The top plot is the summation of the bottom four plots, which shows the outcomes conditional on Charlies and Debbies measurement results.

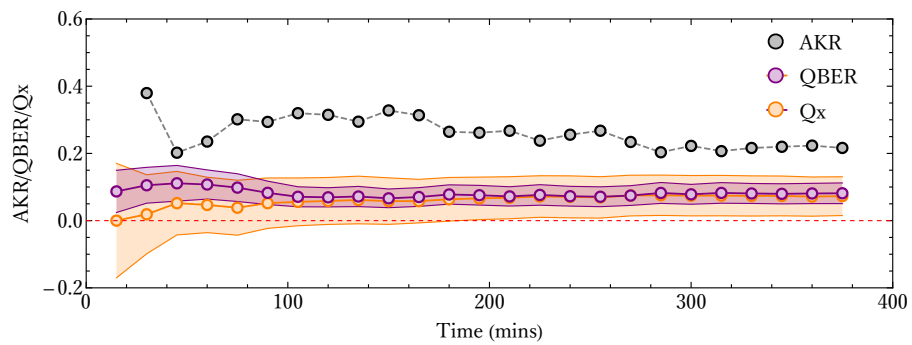


Figure 5.14: Determining $Q_{\mathbb{Z}}$ and $Q_{\mathbb{X}}$ for the 4-photon GHZ state shared by Alice, Bob₁, Bob₂ and Bob₃, and using these results to compute the asymptotic key rate. In order to calculate the asymptotic key rate, Equation (5.5), we first need to calculate $Q_{\mathbb{Z}}$ (QBER) and $Q_{\mathbb{X}}$. This figure shows how the values for all these parameters at a fixed power evolve over time, as more statistics are collected and as the state drifts.

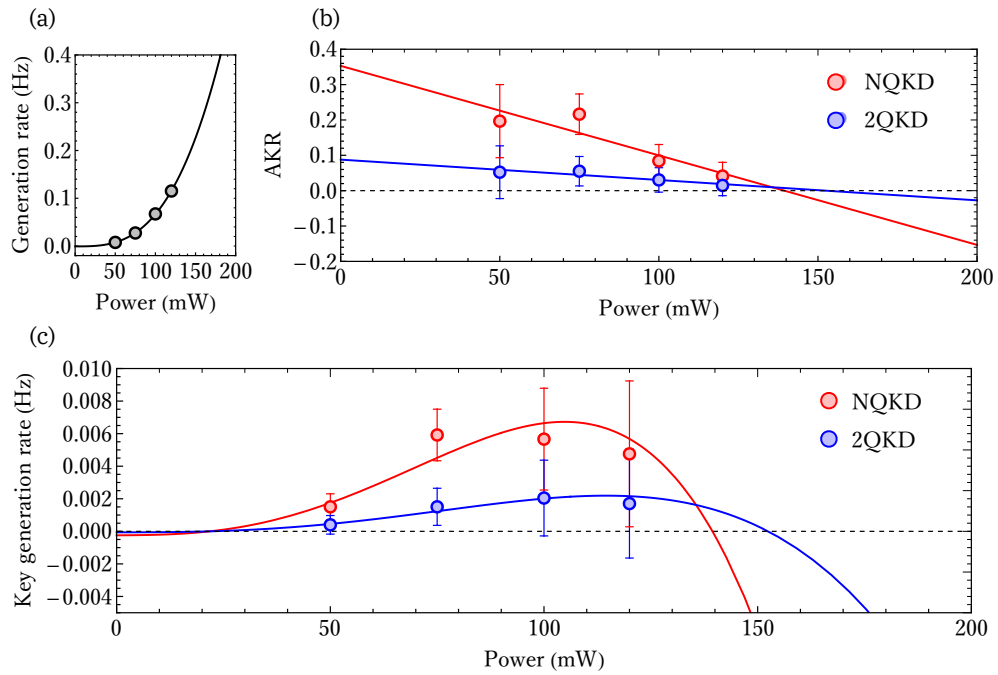


Figure 5.15: Asymptotic key rate and key generation rates for a range of pump powers. The generation rate of our 6-photon state (a) means that the ideal power to operate this protocol at is not simply the highest AKR (b). Due to the scaling of n -fold events from probabilistic sources, there is an optimum position where the scaling of the generation rate, combined with the AKR means that the N-QKD technique operates at an optimal key generation rate (c).

Once we acquire all the measurement settings, encoded with the appropriate single-qubit operations, we perform measurements on the six-photon graph to establish whether we obtain the correct long range correlations that are necessary to evaluate Q_Z and Q_X . Ensuring that the appropriate phase corrections are applied, based on what measurement results Charlie and Debbie obtain and would classically announce, we confirm the correct long-range correlations are obtained for the distilled GHZ state and Bell states. Figures (5.12) and (5.13) show the long range correlations belonging to the GHZ state in the Z and X bases.

Now that we know we can obtain correct correlations for the GHZ state between Alice and all of the Bobs, as well as the required Bell states between the required combination of Alice and Bobs, we can compute Q_Z and Q_X for all the distilled states to complete the parameter estimation step for CKA. Figure (5.14) shows the results from calculations of the AKR, Q_Z and Q_X corresponding to the distilled GHZ state at a pump power of 75mW.

5.2.5.2 AKR

The main result of proof-of-principle network demonstration, is a comparison between the performance of a N-QKD protocol and a 2-QKD protocol using a GME network resource state. Owing to the low count rate, evaluating the ultimate performance of both protocols consists of measuring the noise terms Q_Z and Q_X for parameter estimation and evaluating the respective AKRs.

Figure (5.15) contains all plots constituting our analysis of all protocols we conducted as a function of pump powers. Operating at higher pump power, we see that the probability of generating a six-fold event is much higher, a result of the generation rate scaling as a cubic function. We also see that higher pump powers reduces the AKR, a result of additional noise from multi-photon events, degrading the quality of the state. The non-trivial relation between pump power and AKR, along with the well understood scaling of generation rates with pump power, reveals that an optimal regime to operate this protocol, in terms of conference key rate (product of generation rate and AKR) is not at the lowest pump power, where the AKR is maximum, rather at $\sim 105\text{mW}$. But, this result requires more statistical weighting—which is clear from the magnitude of the error bars that result from poissonian statistics—to offer more conclusive outcomes allowing us to conclude at what power our proof-of-principle protocol will operate most effectively. Negative AKR or more precisely, an $\text{AKR} \leq 0$, physically translates to a regime where there is no extractable key from that round of measurements.

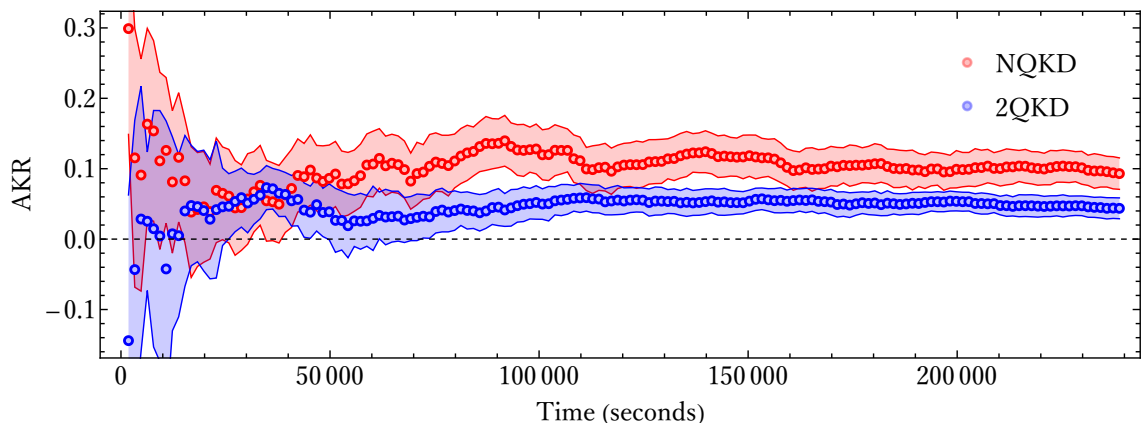


Figure 5.16: Asymptotic key rate at a fixed power over a long measurement period. Measuring the asymptotic key rate over 50 hours worth of measurement time without any correction for drifts in the 6-photon state. This highlights the stability we were able to achieve in the lab. As a consequence of statistics, the results tend towards a ratio of $\text{AKR}_{\text{N-QKD}} : \text{AKR}_{\text{2-QKD}} = 2.13 \pm 0.06$.

We wanted to be absolute in our conclusion that, in a multi-user quantum network scenario (or general quantum network scenario involving GME), the best approach for conducting CKA is to use N-QKD and not 2-QKD primitives. Figure (5.16) shows a measurement with significant statistical weighting. Over 17 days worth of data acquisition time, accumulating nearly 4,000 six-fold events, we conclude that the ratio of CKA key rates is, explicitly, $AKR_{N-QKD} : AKR_{2-QKD} = 2.13 \pm 0.06$. Within this measurement, both canonical approaches (N-QKD rounds and 2-QKD rounds) were performed in 5 minute chunks over the 17 day period, in able to ensure that any drifts in the six-photon state effects the results for the AKR_{N-QKD} and AKR_{2-QKD} symmetrically.

5.3 Concluding remarks

We have shown that key rates for N-QKD primitives over a quantum network based on the distribution of a GME network resource states out performs 2-QKD primitives by more than a factor of 2. We have also shown, for the first time, the generation of a network resource state (in the form of a graph) combined with the successful distillation of smaller entangled resource states between subsets of network users. All of this work constitutes a proof-of-principle demonstration of a quantum network protocol.

The first thing to address about our demonstration is the achieved photon rates. The nature of the six-photon state and the optical arrangement to generate this state made it more vulnerable to multi-photon events entering detection events, reducing the purity of the state and ultimately the terms calculated in parameter estimation. We had made a decision to go to a smaller spot size for the pump, combined with shorter and asymmetric collection distances, a consequence of attempting to obtain eight-fold coincidences for the generate an eight-photon GHZ state. From initial calculations of expected photon rates, to obtain the eight-fold detection rate we wanted, a specific source brightness had to be achieved. This was only achievable with higher effective squeezing via smaller spot sizes in the crystal and shortened collection distances, a consequence of the limited pump power our Ti:Sapph can provide. Based on the discussion from Chapter 3, the reader should be aware that a more relevant metric to use when discussing probabilistic sources is the amount of squeezing applied to the source. We believe that if we change

the source configurations, increasing the spot size of the pump in the crystal and changing collection distances, we can achieve heralding efficiencies—in line with the $> 60\%$ we witnessed in Figure (3.4). Achieving higher heralding would afford us to operate at an effective squeezing equivalent to that we used in this analysis but retain higher key rates. Given the susceptibility to noise from higher-order generation, we could also use temporal multiplexing techniques to up the repetition rate of our Ti:Sapph, from 80MHz to 160MHz. This however will need further reasoning for two reasons. Firstly temporally multiplexing the pump has drastic scaling to multi-photon rates and we do not want to operate in a regime where we do not have enough pump power to exploit the benefits of temporal multiplexing. The second reason is the current operation of our counting logic. We operated on the absolute limit of temporal windows in logic mode to ensure that un-correlated photons from different pulse trains were not affecting measurement results, meaning we believe we have run out of temporal resolution to add another pulse in-between our current pulse train. From preliminary discussions, we believe we can get around this caveat by operating in time-tagging mode and not logic mode, but sample in a smaller discretisation of reading time to reduce the number of photons in the buffer and speed up processing times.

A lot of time will be afforded to developing an in-depth noise model. Understanding how noise effects not only the six-photon state, but also all the possible states we can distill may reveal that a specific distillable state or sets of states may be more robust to characteristic noise. We undertook some preliminary empirical tests to settle a discussion we had about an appropriate noise model. By adjusting the manual phase corrections in each fusion gate we could effectively control the coherence of each of the two-photon interference events. We noticed that populations containing erroneous counts when measuring certain observables would increase whenever we adjusted the manual phase corrections suggesting that a noise model with selective dephasing applied to certain qubits could be appropriate. Furthermore, the asymmetry of the “artificial” noise we introduced by adjusting the phase correction stages in each fusion gate would change the noise parameters Q_Z and Q_X for only a specific distilled Bell pair. This leads onto the next discussion point.

For our analysis, we chose to distill a Bell state between users 1, 2 and 5, 6, then to complete the 2-QKD primitive, we derived a Bell state between users 2,

5. Knowing that there may be some asymmetry in the noise parameters for the distilled Bell states based on the characteristic noise emanating from the optical circuit and resource states, we can explore whether—for the individual Bell state that is required to be shared between two users who have not initially shared a Bell state—there is a better performing Bell state increasing $\text{AKR}_{2\text{-QKD}}$. Alternative Bell states we could have distilled were shown in Figure (5.1).

5.3.1 Acknowledgements

This experiment, and all of the analysis was done with the help of Joseph Ho. I would also like to acknowledge the discussion with Andrés Ulibarrena, Christopher Morrison and Jonathan Webb. Would finally like to acknowledge Massimiliano Proietti and Alessandro Fedrizzi for concieving the project.

Chapter 6

Conclusion

*To read our E-mail, how mean
of the spies and their quantum machine;
Be comforted though,
they do not yet know
how to factorize twelve or fifteen.*

—Volker Strassen
In reply to Jenifer and Peter Shor

Although work follows this conclusion (in the form of an appendix), it is time my writing comes to a close. This thesis contains only some of the work I carried out during my Ph.D, but I believe the work it does contain builds a good narrative which starts with PDC based photon sources that approach absolute ideal operation and finishing with an experiment showcasing these sources by generating a six-photon GME state.

Initially we started this thesis by presenting some basic quantum information science concepts that are used within the thesis and serves as just nomenclature. Then, starting from the most basic equation for the optical response of a material, we showed how one derives the quantum state that governs the PDC process. From there we then introduced the more succinct science contained within this thesis. Engineering the PMF is an absolute necessity in order to attain high purity photons without employing narrow-band filters and we presented an in-depth analysis of the design considerations that must be made to make the final incremental steps to produce the ultimate source of telecom photons. We then characterised the performance of custom designed aKTP crystals with designated design parameters. Our analysis was a true proxy for source performance, interfering photons from separate, but identical crystals. We believe the performance of this source sets a credible benchmark for other PDC sources to outperform. Further, these sources enable investigations

requiring multiple sources that would otherwise be in-achievable without sufficient photon indistinguishability and heralding.

We concluded this thesis with a use case for our sources. Specifically exploiting the high interference visibilities exhibited by photons generated by our aKTP crystals. Maximising the probability of a successful fusion gate, we were able to prepare a six-photon state that is locally equivalent to a specific family of graph states that possess attributes lending them for use as a network resource state. Both the generation and manipulation of graph states has given us invaluable knowledge to develop upon the results we obtained in Chapter 5 and explore other network protocols with other families of graphs. In particular there is scope to implement anonymous CKA [159, 160] as well as loss-resilient conference key agreement, based on redundant encoding and error correction [161] and quantum secret sharing protocols.

Another interesting research direction to explore is adding configurability to graph state generation. The nature of bulk optical arrangements means it is not efficient to have reconfigurable gates without fast switches with feed forward¹. There is scope however to use our photons in commercially available configurable circuits, or photonic processors [162]. Coupled to our ideal photon sources, these configurable circuits could allow us to explore multiple families of graphs.

Beyond just quantum network coding, investigations into measurement device-independent (MDI) protocols could also contribute interesting research to quantum networking tasks. I was always interested in extending the work we did on quantum channel verification in Appendix A. Using the ideas presented in Ref. [163], a GHZ state can be used to perform MDI-QKD. This proposal has already been demonstrated [164], but the prospect remains to implement this with our telecom sources and for different resource states. Additionally, the high heralding efficiencies our source can achieve means we could exploit the lower thresholds on device-independence that were recently derived [165, 166]. The stumbling block, unfortunately something we cannot hurdle ourselves, is the fact we do not possess detectors that operate at $> 90\%$ detection efficiency.

Most discussion in this thesis is focused on discrete variable encoding, however there is a huge amount of ongoing research in continuous variable (CV) encoding. One specific research direction prevalent to the work contained in this thesis is the

¹and a large amount of optical bench space.

use of CV encoding in photonic measurement-based quantum computing architectures that forgo stationary matter based qubits. This paradigm of computation requires a resource state which has sufficient size and is structured correctly. These resource states take the form of a cluster state, of which graph states are a special class of. Currently, there has been impressive experimental work which have generated large 1D and 2D cluster states [167–170]. States are encoded in electric field amplitudes of optical modes that are temporally localised, therefore the size of the state can be huge thanks to the use of time domain multiplexing. There are still several areas of improvements required in order to be able to perform useful universal computations with these states, such as the amount of squeezing, which is still currently below the fault tolerant threshold [171].

Research into deterministic photon sources has also become prevalent, with quantum dots, organic molecules, trapped ions and other solid state structures offering a platform for producing photons on demand [172–177]. Deterministic photon sources are, for obvious reasons, of great interest, and whilst probabilistic PDC sources have underpinned research in quantum information processing for the previous two decades, deterministic photon generation would enable next generation quantum technologies and huge advancements in the capabilities of photonic quantum technologies.

In the introduction we stated that most of the intrinsic limitations of PDC have been removed, but the remaining intrinsic limitation is scalability. Scalability with a probabilistic architecture is fundamentally a tough problem to tackle, with only large scale multiplexing offering a solution. Multiplexing encapsulates a variety of meanings in photon source design, but photon source multiplexing along with feed-forward operations is required to create a pseudo deterministic source [178–184]. Miniaturisation of photon sources is therefore an obvious requirement on the path to scalability, and the development of down-conversion sources within integrated silica-based chips with high photon indistinguishability—such as Ref. [107]—is a large step forward. Highly manufacturable sources promise to be good a candidate for applications that demand large photon numbers, such as fully error-corrected quantum computation. If one could fill a room with a vast amount of these miniature sources, employ efficient multiplexing schemes to overcome the probabilistic stumbling block, and fill what remains of the room with a vast amount of photon number resolving, high efficiency detectors, one could potentially attain a million

qubits for fully error-corrected computation.

Appendix 1:

Measurement-device-independent verification of quantum channels

As mentioned through this thesis, the future structure of quantum networks is a prevalent area of research. What is absolute however, is that entanglement in some form will be distributed to network users attached via some quantum channel. There is a need therefore, to certify that an unknown channel acts as an entanglement-preserving channel. The narrative supporting the importance of being able to verify whether a channel is capable of preserving entanglement, comes from the stance of a skeptic, who has been given a quantum channel to use to establish correlations with another user of a network, but does not necessarily trust the operators of the network. This work seeks to outline a means by which a skeptic could characterise the performance of a channel without requiring a resource intensive tomographic reconstruction of the channels process matrix. To verify the channel in a minimal way, we lean on the notions of semi-quantum games [185] and entanglement witnesses [163] in order to perform a verification protocol in a measurement-device-independent fashion (MDI), where the skeptic has to lay trust in only their state preparation device. Additionally, this scheme is adaptable to quantum memory verification, as it was first proposed in Ref.[186].

Measurement-Device-Independent Verification of Quantum ChannelsFrancesco Graffitti^{1,*}, Alexander Pickston,¹ Peter Barrow,¹ Massimiliano Proietti,¹ Dmytro Kundys¹,Denis Rosset,² Martin Ringbauer³, and Alessandro Fedrizzi¹¹*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences,
Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*²*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, Ontario, Canada N2L 2Y5*³*Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, A-6020 Innsbruck, Austria*

(Received 28 June 2019; published 2 January 2020)

The capability to reliably transmit and store quantum information is an essential building block for future quantum networks and processors. Gauging the ability of a communication link or quantum memory to preserve quantum correlations is therefore vital for their technological application. Here, we experimentally demonstrate a measurement-device-independent protocol for certifying that an unknown channel acts as an entanglement-preserving channel. Our results show that, even under realistic experimental conditions, including imperfect single-photon sources and the various kinds of noise—in the channel or in detection—where other verification means would fail or become inefficient, the present verification protocol is still capable of affirming the quantum behavior in a faithful manner with minimal trust on the measurement device.

DOI: [10.1103/PhysRevLett.124.010503](https://doi.org/10.1103/PhysRevLett.124.010503)

The ability to transmit and store quantum states and coherently manipulate the timing of photonic signals is a crucial requirement in quantum technologies [1]. Quantum communication links in combination with quantum memories form the quantum channels that offer these capabilities. These quantum channels thus play a pivotal role in enabling full scale quantum networks [2], promising unconditionally secure communication and the prospect of distributed quantum computing.

With the development of such quantum channels, especially quantum memories, comes the challenge of certifying their capabilities [3,4]. In particular, we seek the ability to discern a truly nonclassical channel from a cheap knock-off, such as a channel that simply measures the input state and approximately reprepares it at the output. While the latter could preserve some information about the state, it cannot preserve the exact quantum state nor any previously established correlations, rendering it useless for quantum applications. We denote channels of this sort as entanglement breaking (EB), in contrast to true quantum memories or coherent quantum channels, which preserve entanglement at least to some extent.

Consider an unknown channel that is claimed to be nonclassical, i.e., entanglement preserving. The most straightforward approach to obtain a complete characterization of the channel is a tomographic reconstruction of the channel's process matrix [5]. In practice, however, this approach is too resource intensive for all but low-dimensional channels, and further requires precise control and trust in all parts of the experiment. In most cases, such trust is undesirable or cannot be guaranteed at all. One way

to overcome this is by using the correlations of entangled quantum systems, where a violation of a Bell inequality certifies the presence of entanglement even when the measurements are performed by untrusted black-box devices. Consequently, when considering an ideal scenario, Bell-test-based protocols allow for the verification of quantum channels in a so-called *device-independent* (DI) way, that is without requiring any trust in the experimental devices [6] even provide guarantees on the quality of the channel via self-testing [7]. On the flip side, these approaches cannot capture all nonclassical channels [8] and are subject to challenging loopholes [9–11] that make them very fragile to losses and experimentally difficult to implement. Moreover, in practice we rarely face the situation where nothing can be trusted such that a fully device-independent approach is necessary. Instead, while we might face an untrusted measurement device, we typically have access to a trust-worthy state preparation device allowing us to generate well-defined quantum states of our choice: a scenario commonly referred to as measurement-device-independent (MDI).

MDI schemes were first proposed in the context of quantum key distribution [12], and then applied to entanglement verification [13] for spatially separated subsystems within the framework of semiquantum games [14,15], providing several advantages over Bell tests [16]. These methods have since been extended to quantum steering [17] and to the analysis of entanglement structure [18] and its quantification [19–21], which has been demonstrated experimentally [22–24]. However, these schemes were solely focused on probing correlations within quantum

states. More recently, it was shown that MDI approaches and semiquantum games can be repurposed to test the quantum properties of a channel, e.g., in situations where one party wants to test another party's ability to maintain the quantum properties of a system over time [11], such as in a quantum memory.

Here we demonstrate experimentally that MDI verification of quantum channels is a simple technique that is highly robust to experimental imperfections and viable with current technology. We study the performance and success probability of the method for channels suffering from depolarizing and dephasing noise, taking into account all experimental imperfections (such as imperfect state preparation when multiple copies of the input state are prepared), a problem that so far has not received sufficient attention. Under all conditions achievable with current technology, we find that the MDI approach outperforms Bell-test-based techniques in terms of resource requirements as well as noise resilience without the need for extra assumptions such as fair sampling. This method can thus certify a much wider range of channels and remains practical under realistic experimental conditions.

We now consider a typical experimental scenario, where a client (Alice) wishes to test a potentially dishonest quantum memory (provided by Bob) before deployment in a quantum network. Alice is assumed to possess a trusted preparation device, which is a scenario that naturally lends itself to the use of semiquantum games. Here, Alice repeatedly asks Bob a set of randomized "questions" by sending him quantum states and gets back a classical answer from Bob in every round. Bob is then asked to maximize a payoff function chosen to witness whatever quantum property Bob claims to possess. Since the questions are nonorthogonal, Bob merely knows the set of possible questions, but cannot know which question is asked in each round and thus cannot cheat. This method thus allows Alice to witness whether Bob possesses the claimed quantum property without having to trust him.

In each round, Alice sends successively two questions with a time delay between them, which forces Bob to store the first question until the second one arrives. In our notation, the first question is a state chosen at random from a finite set $\{\xi_x\}$ indexed by x , while the second question is chosen from a finite set $\{\psi_y\}$ indexed by y ; both questions are sampled with uniform probability. After receiving the second question, Bob returns a classical answer b back to Alice. Bob is asked to maximize a prearranged payoff function $\omega(b, x, y)$ using the quantum channel \mathcal{N} at his disposal. In analogy with Bell scenarios, we write the payoff then achieved $W = \sum_{bxy} \omega(b, x, y) P(b|xy)$. The combination of the coefficients $\omega(b, x, y)$ with the sets $\{\xi_x\}$ and $\{\psi_y\}$ is a temporal semiquantum game [11]. Every such game has an upper bound W_{EB} on the payoff achievable when Bob has only an entanglement-breaking channel at its disposal.

In our experiment, the sets $\{\xi_x\}$ and $\{\psi_y\}$ are identical and composed of symmetric informationally complete single-qubit quantum states which form a nonorthogonal basis of the Hilbert space with constant pairwise overlap of $1/3$ [25]. As shown in the Supplemental Material [26], other set of states can be chosen for the protocol with some implementation benefits. Nonorthogonality ensure that, although Bob knows the set of possible questions, he cannot with certainty know which questions are being asked in each round of the game. We write $x, y = 0, 1, 2, 3$ the indices of these two successive questions ξ_x, ψ_y sent to Bob, while Bob sends back a classical answer $b = 0, 1$. The property we are testing is a claim made by Bob that he possesses a nonentanglement-breaking channel corresponding to a Choi matrix Φ [28]. Accordingly, this Choi matrix is entangled, a fact that can be tested by an entanglement witness [29] F such that $\text{tr}[F\Phi] > 0$ while $\text{tr}[F\Phi_{\text{EB}}] \leq 0$ for Choi matrices of entanglement-breaking channels. Our payoff coefficients $\omega(b, x, y)$ are chosen so that $\omega(b = 1, x, y) = 0$, while $\omega(b = 0, x, y)$ provides a decomposition of that witness $F = \sum_{xy} \omega(0, x, y) (\xi_x^\top \otimes \psi_y^\top)$. This ensures [11] that $W_{\text{EB}} = 0$ while $W > 0$ when Bob actually implements the channel he claims to possess and projects the joint two-photon state onto a singlet state $|\Psi^-\rangle$. In each round, Bob announces his result b to Alice, who computes the payoff using her knowledge of the prepared questions. We studied the effects of an imperfect quantum channel by simulating additional depolarizing noise \mathcal{N}_p or dephasing noise \mathcal{N}_ϕ , defined as

$$\begin{aligned} \mathcal{N}_p(\rho) &= (1-p)\rho + p\mathbb{1}/2, \\ \mathcal{N}_\phi(\rho) &= \left(1 - \frac{p}{2}\right)\rho + \frac{p}{2}\sigma_3\rho\sigma_3, \end{aligned} \quad (1)$$

where $\mathbb{1}$ and σ_3 are the identity and Pauli Z operator, respectively, and $0 \leq p \leq 1$ is the noise strength. In both cases, the optimal payoff coefficients are found to be

$$\begin{aligned} \omega(b = 0, x, y) &= \begin{cases} -5/8 & \text{if } x = y \\ 1/8 & \text{otherwise} \end{cases} \\ \omega(b = 1, x, y) &= 0, \end{aligned} \quad (2)$$

where $b = 0$ corresponds to a successful projection of the joint state onto the singlet state and $b = 1$ to any other measurement outcome.

The experiment was implemented with the setup shown in Fig. 1(a). Pairs of 1550 nm single photons are generated via degenerate parametric down-conversion (PDC) in a custom-poled potassium titanyl phosphate (KTP) crystal [30,31] pumped by 775 nm, 1.6 ps pulses with 80 MHz repetition rate, and 75 mW of average pump power, focused to a beam waist of 350 μm . After being separated from the pump with a dichroic mirror (DM), one photon of each pair is loosely filtered, transmitted on a polarizing beam-splitter

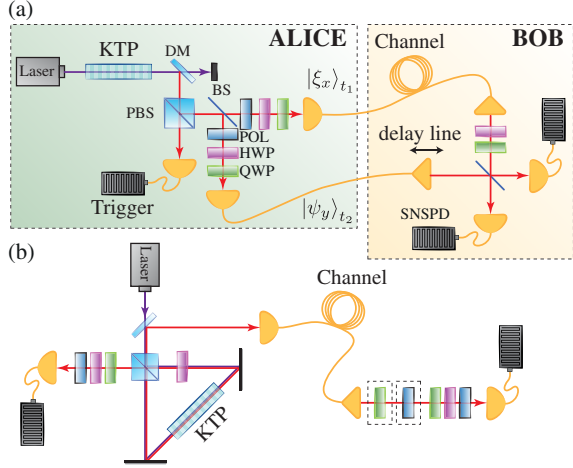


FIG. 1. Experimental setup. (a) MDI entanglement witness setup: the left-green (right-yellow) shading indicates the trusted (untrusted) parts of the experiment. (b) Untrusted channel verification setup via Bell test.

(PBS), and detected by a superconducting nanowire single-photon detector (SNSPD, 80% nominal quantum efficiency, ~ 200 Hz dark counts), providing the heralding signal for its twin photon. We benchmark the source by sending the downconverted photons directly to the SNSPDs, bypassing Bob's part of the setup. We measure a brightness of 140 kHz detected coincident counts and 65% heralding efficiency.

Alice encodes a probe state ξ_x in the heralded photon using a sequence of a polarizer (POL), half-wave (HWP), and quarter-wave plate (QWP). This probe state represents the first question in our semiquantum game, which Bob receives at time t_1 , and is asked to process in his alleged quantum channel. Bob's quantum channel is a 15 m single-mode fiber emulating a quantum memory with fixed storage time of ~ 75 ns: this value exceeds the SNSPD's reset time (~ 50 ns), the minimum time interval required by Alice's source to herald a second photon. An HWP and a QWP are used to implement a noisy channel with variable noise-strength p by applying a combination of Pauli operators according to Eq. (1) for a measurement time proportional to p . At a later time t_2 , Alice prepares in the same way a second probe state ψ_y —corresponding to the second question in the game—and sends it to Bob, who is asked to perform a joint measurement on the two states via two-photon interference on a beam splitter (BS) and broadcast the outcome. Bob uses a tunable delay line to synchronize the two photons' arrival time at the BS: only a coincidence click event of the detectors after the BS corresponds to $b = 0$ in Eq. (2) (i.e., a successful projection on the singlet state), while any other event corresponds to $b = 1$.

Unlike the MDI protocol described above, a Bell-test approach, i.e., a fully device-independent verification of a quantum channel requires Alice to prepare entangled

quantum state. We produce entangled pairs of photons ($99.34^{+0.01}_{-0.09}\%$ purity and $99.62^{+0.01}_{-0.04}\%$ fidelity with the Ψ^- state) via PDC in Sagnac interferometric scheme [32], as shown in Fig. 1(b). Alice then sends one photon of the entangled pair to Bob, who sends it through his channel. An additional set of HWP, QWP, and POL is used to introduce controllable dephasing and depolarizing noise. After the stored photon has been retrieved, a Clauser-Horne-Shimony-Holt Bell test [33] is performed on the joint system, and a violation of the inequality guarantees the genuine quantumness of the channel.

Figure 2(a) shows the result of our MDI channel verification for dephasing and depolarizing noise compared to a Bell-test approach with fair sampling assumption (i.e., neglecting the losses in the untrusted part of the setup). We show that, even in this idealized scenario, the MDI

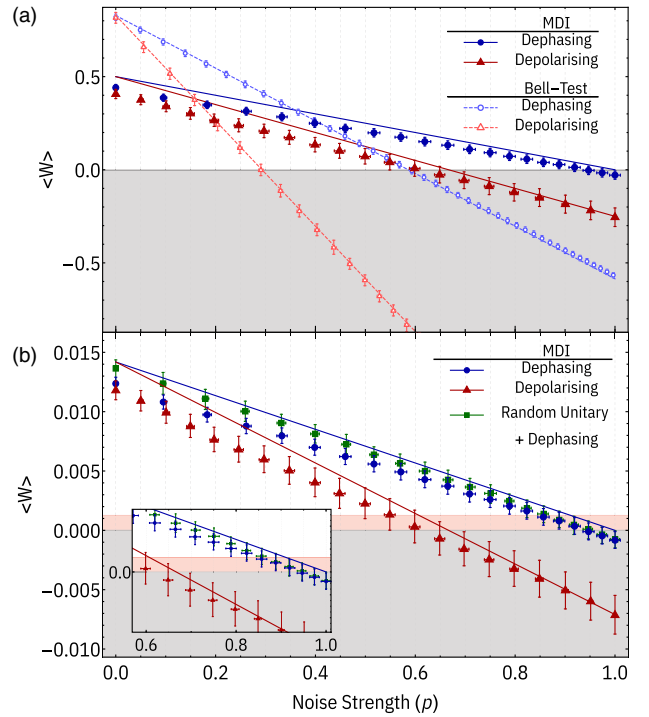


FIG. 2. Experimental results. MDI entanglement witness measures (a) with and (b) without fair sampling assumption. Lines and points represent the theoretical prediction and the experimental data, respectively. The gray-shaded area corresponds to entanglement-breaking channels, while the red-shaded area represents the actual threshold for entanglement-breaking channels, taking into account Bob's optimal cheating strategy. The discrepancy between theory prediction and data points is mainly due to imperfect two-photon interference on Bob's BS (we estimate a Bell-state measurement fidelity $\lesssim 95\%$). Note that the theoretical lines are computed for illustration purposes only using the full knowledge of the setup and therefore would not be available to Alice in the actual implementation of the protocol. The error bars in the data points represent 3σ statistical confidence regions obtained via Monte Carlo resampling ($n = 10^5$) assuming a Poissonian photon-counting distribution.

approach outperforms the Bell test as it can certify quantumness for larger noise strength than the Bell test (where the magnitude of noise each experimental approach can tolerate is computed from the intersection of the average payoff with the EB threshold). In theory, the quantum nature of the depolarizing channel can be witnessed up to a noise level of $p < 2/3$, while the Bell-based tests can only certify the channel up to $p \sim 0.29$. Surprisingly, the quantumness of a dephasing channel can be certified for any finite amount of noise, while a Bell-test approach can at best verify the channel up to $p \lesssim 0.58$. Crucially, under ideal experimental conditions—i.e., no loss and perfect single photon sources—the best strategy Bob can use to convince Alice that he is in possession of a genuine quantum channel is to truthfully reveal the result of the joint measurement. Any other tactic would not maximize the payoff function [11].

In order to guarantee device independence, the Bell-test approach would require very high detection efficiencies that are at best at the limit of current technical capabilities. The MDI approach, on the other hand, is less demanding in terms of experimental requirements. The effects of losses and imperfections on our protocol are twofold. First, lost photons lead to a decreased payoff, and second, Bob can exploit imperfections to cheat. Studying the latter possibility in some more detail, we note that most state-of-the-art photon sources suffer from a small probability of emitting multiple photons at a time, which Bob can exploit to extract information about the questions sent by Alice. Bob could then use this information to artificially inflate the payoff function by the following strategy: whenever he gets no more than one photon in each question, he announces an unsuccessful projection on the singlet state (i.e., $b = 1$). If he gets more than one photon in one of the questions and at least one in the other one, he can gather information on the question itself and perform a conveniently chosen local operation and classical communication (LOCC) positive-operator valued measure (POVM) to furtively inflate his payoff. In the Supplemental Material [26], we derive the maximal payoff that Bob could achieve with an EB channel using these strategies and the known characteristics of Alice’s photon source. By using this new threshold in our protocol, we can reliably, and without further assumptions, certify whether a channel is quantum, even if Bob is actively trying to cheat. Figure 3 shows the theoretical trade-off between losses, noise, and protocol success for depolarizing noise at a fixed performance of the trusted source (given by the ratio of multiphoton emissions: the red area above the threshold represents the parameters space’s region where secure certification of the channel’s quantumness can be achieved).

Taking into account both losses and multiphoton emissions according to our experimental parameters—overall heralding efficiency of $\sim 17\%$ and multiphoton contribution of $\sim 0.25\%$ —puts us in a regime far beyond where a fully DI approach would apply due to its sensitivity to loss. On the other hand, the MDI protocol reveals itself to be

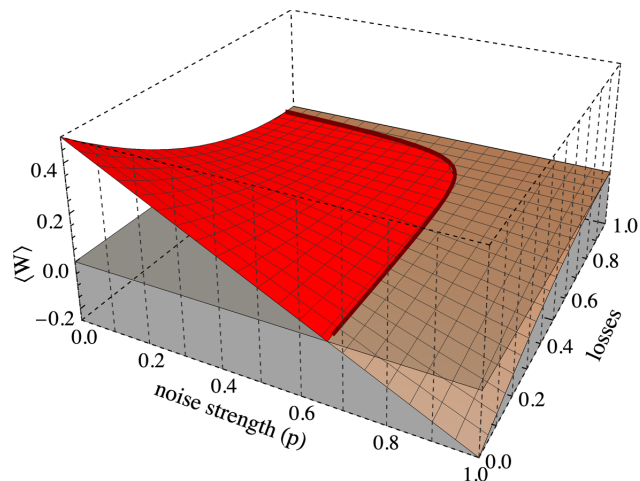


FIG. 3. MDI channel verification tradeoffs. Shown is the ideal expectation value $\langle W \rangle$ of an MDI entanglement witness for an identity channel with depolarizing noise of strength p and different amounts of loss. The multiphoton contribution is fixed at $\sim 0.25\%$, as in our experimental setup, and results in a decreased size of the parameter region where certification of quantum behavior is possible.

significantly more robust to such experimental imperfections, being still capable of certifying the nature of a quantum channel, as we show in Fig. 2(b).

So far, we have discussed MDI certification of a noisy identity channel. In practice, an imperfect channel might also apply some unknown unitary rotation to the stored qubit. In this case, a nominally entanglement-preserving channel might appear to be EB due to the wrong choice of witness or payoff. In order to verify such channels, Alice uses a modified protocol, where she splits the answers obtained from Bob into two sets. The first set is used to reconstruct the channel’s process matrix via quantum process tomography and then computing the corresponding entanglement witness (as discussed, e.g., in Ref. [29] or in the Supplemental Material [26]). Alice can then perform the standard MDI verification with the adapted witness on the second dataset. Since only the second stage of this extended protocol is MDI, Bob could attempt to cheat in the first stage. However, all this would achieve is that Alice computes a suboptimal witness, which inevitably lowers the achievable payoff in the second stage. Bob’s best strategy to have his channel certified is thus to broadcast the true outcome of the joint measurement he performs while Alice performs the process tomography of the channel, so that she can build the optimal witness for the channel at hand.

Experimentally, the unknown unitary rotation was implemented by means of an HWP and a QWP at the output of the channel, and the MDI protocol was performed in the context of certifying its quantumness in the presence of dephasing noise. The results are shown in Fig. 2(b) with losses and multiphoton corrections taken into account. We

note that this protocol behaves as the standard MDI protocol for the identity channel, confirming the suitability of using a MDI approach in more complex scenarios where nontrivial noisy channels are involved.

Discussion.—We have provided a readily accessible MDI recipe for verifying a quantum channel with sustained performance in the presence of noise and loss much beyond the capabilities of fully DI methods, with the minimum possible set of assumption on the device under examination. With minimal demands on the trusted side (i.e., a single photon source), this method is ideally suited as a dependable benchmark for quantum memories and more general quantum channels. With the future vision of large scale quantum networks, this type of verification protocol can be a powerful tool for a security-conscious user of the network, who does not necessarily trust the third party operating the network. A natural extension of this work would be probing different properties of a quantum memory simultaneously. Fidelity, storage time and recall properties could be tested by changing the timing between the probe photons. On the theory side, the protocol could be extended to quantify the quantum nature of the channel instead of verifying it as has been done for the MDI quantification of entanglement [19–21]; in this direction, one would need to use a capacity that quantifies specifically the quantum part of the channel: the negativity of the channel Choi state, or the quantum relative entropies [34] could be used for that purpose.

This work was supported by the UK Engineering and Physical Sciences Research Council (Grant No. EP/N002962/1). F. G. acknowledges studentship funding from EPSRC under Grant No. EP/L015110/1. This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant No. 801110 and the Austrian Federal Ministry of Education, Science and Research (BMBWF). It reflects only the author’s view; the EU Agency is not responsible for any use that may be made of the information it contains. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

Note added in the proof.—Recently, we became aware of this Letter we became aware of similar work that has been recently carried out [35]. The work in this Letter implements a similar protocol, but in a different regime of encoding.

*Corresponding author.
fraccalo@gmail.com

[1] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, Linear optical quantum computing with photonic qubits, *Rev. Mod. Phys.* **79**, 135 (2007).

- [2] H. J. Kimble, The quantum internet, *Nature (London)* **453**, 1023 (2008).
- [3] C. Macchiavello and M. Rossi, Quantum channel detection, *Phys. Rev. A* **88**, 042335 (2013).
- [4] M. F. Pusey, Verifying the quantumness of a channel with an untrusted device, *J. Opt. Soc. Am. B* **32**, A56 (2015).
- [5] G. M. D’Ariano and P. Lo Presti, Quantum Tomography for Measuring Experimentally the Matrix Elements of an Arbitrary Quantum Operation, *Phys. Rev. Lett.* **86**, 4195 (2001).
- [6] J.-D. Bancal, N. Gisin, Y.-C. Liang, and S. Pironio, Device-Independent Witnesses of Genuine Multipartite Entanglement, *Phys. Rev. Lett.* **106**, 250404 (2011).
- [7] J.-D. Bancal, K. Redeker, P. Sekatski, W. Rosenfeld, and N. Sangouard, Device-independent certification of an elementary quantum network link, [arXiv:1812.09117](https://arxiv.org/abs/1812.09117).
- [8] R. Pal and S. Ghosh, Non-locality breaking qubit channels: The case for CHSH inequality, *J. Phys. A* **48**, 155302 (2015).
- [9] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [10] E. Santos, Critical analysis of the empirical tests of local hidden-variable theories, *Phys. Rev. A* **46**, 3646 (1992).
- [11] D. Rosset, F. Buscemi, and Y.-C. Liang, Resource Theory of Quantum Memories and their Faithful Verification with Minimal Assumptions, *Phys. Rev. X* **8**, 021033 (2018).
- [12] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [13] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin, Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States, *Phys. Rev. Lett.* **110**, 060405 (2013).
- [14] F. Buscemi, All Entangled Quantum States are Nonlocal, *Phys. Rev. Lett.* **108**, 200401 (2012).
- [15] L. Guerini, M. T. Quintino, and L. Aolita, Distributed sampling, quantum communication witnesses, and measurement incompatibility, *Phys. Rev. A* **100**, 042308 (2019).
- [16] D. Rosset, C. Branciard, N. Gisin, and Y.-C. Liang, Entangled states cannot be classically simulated in generalized Bell experiments with quantum inputs, *New J. Phys.* **15**, 053025 (2013).
- [17] E. G. Cavalcanti, M. J. W. Hall, and H. M. Wiseman, Entanglement verification and steering when Alice and Bob cannot be trusted, *Phys. Rev. A* **87**, 032306 (2013).
- [18] Q. Zhao, X. Yuan, and X. Ma, Efficient measurement-device-independent detection of multipartite entanglement structure, *Phys. Rev. A* **94**, 012343 (2016).
- [19] F. Shahandeh, M. J. W. Hall, and T. C. Ralph, Measurement-Device-Independent Approach to Entanglement Measures, *Phys. Rev. Lett.* **118**, 150505 (2017).
- [20] I. Šupić, P. Skrzypczyk, and D. Cavalcanti, Measurement-device-independent entanglement and randomness estimation in quantum networks, *Phys. Rev. A* **95**, 042340 (2017).
- [21] D. Rosset, A. Martin, E. Verbanis, C. C. W. Lim, and R. Thew, Practical measurement-device-independent entanglement quantification, *Phys. Rev. A* **98**, 052332 (2018).
- [22] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Implementation of a

- Measurement-Device-Independent Entanglement Witness, *Phys. Rev. Lett.* **112**, 140506 (2014).
- [23] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, Experimental measurement-device-independent entanglement detection, *Sci. Rep.* **5**, 8048 (2015).
- [24] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Resource-Efficient Measurement-Device-Independent Entanglement Witness, *Phys. Rev. Lett.* **116**, 190501 (2016).
- [25] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, Symmetric informationally complete quantum measurements, *J. Math. Phys. (N.Y.)* **45**, 2171 (2004).
- [26] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.124.010503> for details on the semiquantum game, which includes the additional Ref. [28].
- [27] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Complete family of separability criteria, *Phys. Rev. A* **69**, 022308 (2004).
- [28] M. Jiang, S. Luo, and S. Fu, Channel-state duality, *Phys. Rev. A* **87**, 022310 (2013).
- [29] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep.* **474**, 1 (2009).
- [30] F. Graffitti, D. Kundys, D. T. Reid, A. M. Brańczyk, and A. Fedrizzi, Pure down-conversion photons through sub-coherence-length domain engineering, *Quantum Sci. Technol.* **2**, 035001 (2017).
- [31] F. Graffitti, P. Barrow, M. Proietti, D. Kundys, and A. Fedrizzi, Independent high-purity photons created in domain-engineered crystals, *Optica* **5**, 514 (2018).
- [32] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, A wavelength-tunable fiber-coupled source of narrowband entangled photons, *Opt. Express* **15**, 15377 (2007).
- [33] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, *Phys. Rev. Lett.* **23**, 880 (1969).
- [34] X. Yuan, Hypothesis testing and entropies of quantum channels, *Phys. Rev. A* **99**, 032317 (2019).
- [35] Y. Mao, Y.-Z. Zhen, H. Liu, M. Zou, Q.-J. Tang, S.-J. Zhang, J. Wang, H. Liang, W. Zhang, H. Li, L. You, Z. Wang, L. Li, N.-L. Liu, K. Chen, T.-Y. Chen, and J.-W. Pan, preceding Letter, Experimentally Verified Approach to Nonentanglement-Breaking Channel Certification, *Phys. Rev. Lett.* **124**, 010502 (2019).

Appendix 2: Direct generation of pulsed-mode entanglement

Rather than targeting a gaussian PMF, one could target more exotic functions, although there is a restriction on what functions can be tracked. Within a footnote in Chapter 3, we mentioned that our domain engineering technique combined with a suitable tracking algorithm could be used to design crystals with PMFs that have non-Gaussian PMFs. Thus, the technique has now been used for efficient generation of time-frequency mode entanglement [94] and time-frequency hyperentanglement [95]. The following work, Ref. [94] is what follows in this Appendix.

In the case where we want to generate time-frequency mode entanglement, Equation (3.3) from Chapter 3 is replaced with the following,

$$\phi_{\text{target}}(\Delta k) = 2(\Delta k - \Delta k_0)\sigma e^{-\frac{1}{2}(\Delta k - \Delta k_0)^2\sigma^2}. \quad (6.1)$$

Rather than using the same tracking algorithm outlined in Section 3.1.3, a finer discretisation of the domain structure is required. We therefore use the algorithm from Ref. [92], that allows domain widths smaller than the coherence length ℓ_c . As we stated in our discussion of tracking algorithms, smaller domain widths are ideal for shorter length crystals phase-matched for shorter temporal pulses and for tracking functions that contain more features, such as Hermite-Gauss modes.

Direct Generation of Tailored Pulse-Mode Entanglement

Francesco Graffitti^{1,*}, Peter Barrow^{1,†}, Alexander Pickston¹, Agata M. Brańczyk², and Alessandro Fedrizzi¹

¹*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

²*Perimeter Institute for Theoretical Physics, Waterloo, Ontario N2L 2Y5, Canada*



(Received 3 October 2019; accepted 13 January 2020; published 4 February 2020)

Photonic quantum technology increasingly uses frequency encoding to enable higher quantum information density and noise resilience. Pulsed time-frequency modes (TFM) represent a unique class of spectrally encoded quantum states of light that enable a complete framework for quantum information processing. Here, we demonstrate a technique for direct generation of entangled TFM-encoded states in single-pass, tailored down-conversion processes. We achieve unprecedented quality in state generation—high rates, heralding efficiency, and state fidelity—as characterized via highly resolved time-of-flight fiber spectroscopy and two-photon interference. We employ this technique in a four-photon entanglement swapping scheme as a primitive for TFM-encoded quantum protocols.

DOI: [10.1103/PhysRevLett.124.053603](https://doi.org/10.1103/PhysRevLett.124.053603)

Generating entanglement in intrinsically high-dimensional degrees of freedom of light, such as transverse and longitudinal spatial modes [1,2], or time and frequency, constitutes a powerful resource for photonic quantum technologies—photons that carry more information enable more efficient protocols [3,4]. Time-frequency encoding is intrinsically suitable for waveguide integration and fiber transmission [5,6], making it a promising choice for practical, high-dimensional quantum applications. Quantum information can be encoded either in discrete temporal or spectral modes (namely time- and frequency-bin encoding [6–9]) or in the spectral envelope of the single-photon wave packets—time-frequency mode (TFM) encoding [5,10]. TFM-encoded states arise naturally in parametric down-conversion (PDC) sources, as TFMs are eigenstates of the PDC process and they span an infinite-dimensional Hilbert space. Conveniently, TFMs possess highly desirable properties: being centered around a target wavelength makes them compatible with fiber networks, they are robust against noise [11] and chromatic dispersion [12], their pulsed nature enables synchronization and therefore multiphoton protocols and they offer intrinsically high dimensionality [10]. Manipulation and detection of TFMs is enabled by the quantum-pulse toolbox, where sum- and difference-frequency generation are used for reshaping and projecting the quantum states [5,10]. However, generating entangled TFMs in a controlled way can be very challenging [13–17], limiting their usefulness in realistic scenarios. Here, we overcome this problem exploiting domain-engineered nonlinear crystals [18,19] for generating TFM entanglement from standard ultrafast laser pulses in a single-pass PDC experiment. We experimentally validate this technique by benchmarking a maximally antisymmetric state at telecom wavelength with near unity fidelity, and implement a four-photon entanglement swapping scheme. Our work

complements the pulse-gate toolbox [5,10] for TFM quantum information processing, and establishes a standard for the generation of TFM quantum states of light while paving the way for more complex frequency encoding.

In a PDC process, a pump photon probabilistically down-converts into two photons under momentum and energy conservation. The second-order nonlinearity of a crystal mediates the process through the phase-matching function (PMF) which, together with the pump spectral profile, dictates the spectral properties of the output biphoton state in the form of its joint spectral amplitude (JSA). The spectral entanglement between the PDC photons is quantified by the Schmidt number via Schmidt decomposition of the JSA [20]: a separable, unentangled JSA has a Schmidt number of 1; higher values indicate the presence of entanglement. Conveniently, this decomposition also provides the spectral modal structure of the PDC biphoton state. TFMs can therefore be engineered by shaping the JSA, either by modifying the pump-pulse amplitude function [10] or, as we demonstrate here, by shaping the PMF via nonlinearity engineering. Domain-engineered crystals have been employed successfully for the generation of spectrally pure heralded photons [18,19], where undesired frequency correlations are eliminated by tailoring a Gaussian nonlinearity profile. Here we extend this technique to the direct, controlled generation of custom TFM entanglement.

We use the Hermite-Gauss modes [10] basis to encode the TFM quantum state, with the goal of generating the maximally entangled antisymmetric Bell state:

$$|\psi^-\rangle_{s,i} = \frac{1}{\sqrt{2}} (|\wedge\rangle_s |\vee\rangle_i - |\vee\rangle_s |\wedge\rangle_i), \quad (1)$$

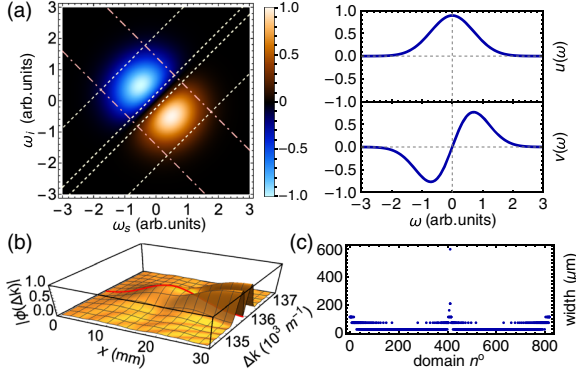


FIG. 1. Crystal engineering. (a) Maximally entangled JSA (left) and corresponding TFM basis states, $u(\omega)$, $v(\omega)$ (right). The pink dot-dashed lines and the yellow dashed lines are the $1/e$ contours of the pump's and PMF's amplitudes, respectively. (b) Target phase-matching function along the crystal at different momentum mismatch (ΔK) values: the tracking algorithm chooses the domain orientation to track the PMF at the quasi-phase-matching condition $\Delta K = \Delta K_0$, as shown by the red trace. (c) Target crystal domain structure.

where “s” (“i”) labels the signal (idler) photon. The state (1) corresponds to the joint spectrum encoded in the TFM basis states $\wedge = u(\omega)$ and $\vee = v(\omega)$ in Fig. 1(a) (see the Supplemental Material [21], Sec. 1 for details on the biphoton spectral structure). We use our recently developed nonlinearity-engineering algorithm [18] to shape the PMF [$\phi(x, \Delta k)$] as a first-order Hermite-Gauss function. We design a 30 mm potassium titanyl phosphate (KTP) crystal for symmetric group-velocity matching with a 1.3 ps laser pulse [20]. The fundamental domain width is $\sim 23.1 \mu\text{m}$, equal to the coherence length of a 775 nm pump down-converted into two 1550 nm photons. Our algorithm chooses the ferroelectric orientation of individual domains to track a target PMF along the field propagation in the crystal (see the Supplemental Material [21], Sec. 2 for details on the algorithm). Figures 1(b) and 1(c) show the resulting PMF [$\phi(\Delta k)$ at $x = 30 \text{ mm}$] and the required crystal domain configuration.

The designed crystal was manufactured commercially by *Raicol Ltd.* We set up a collinear PDC source [19], where a 80 MHz, pulsed Ti:sapphire laser is focused into the tailored KTP crystal to create orthogonally polarized photon pairs via type-II PDC. The photons are loosely filtered with a bandpass filter (~ 3 times broader than the PDC photons' bandwidth). A polarizing beam splitter separates the PDC photons before they are coupled into single-mode fibers. We measured a source brightness of $\sim 4 \text{ KHz/mW}$ photon pairs with a symmetric heralding efficiency $> 60\%$, a reasonable trade-off achieved by optimizing the pump, signal, and idler focusing conditions [19].

A full characterization of the biphoton quantum state could be obtained via quantum state tomography in the TFM basis, which requires projective measurements onto

three mutually unbiased bases using cascades of tailored nonlinear processes [22–24], or by reconstructing the JSA including its phase, which assumes a pure biphoton state and involves complex interferometric techniques [25–27]. We instead characterize the PDC state using an indirect approach that exploits joint spectral intensity (JSI) reconstruction via dispersive fiber spectroscopy [28] and two-photon interference [Hong-Ou-Mandel (HOM) effect [29]] to infer information on the populations and the entanglement of the quantum state, respectively.

The setup for the JSI reconstruction is shown in Fig. 2(a) (modes I). Each photon is sent through a $\sim 20 \text{ km}$ single-mode fiber to convert spectral to temporal information exploiting the fiber dispersion of $\sim 18 \text{ ps/km/nm}$ at 1550 nm. The photons are then detected with superconductive nanowire single photon detectors (SNSPD), with $\sim 80\%$ detection efficiency and $< 50 \text{ ps}$ timing jitter. Arrival times are recorded as time tags by a *Picoquant HydraHarp* in 1 ps bins for offline processing. We collected $\sim 2.8 \times 10^6$ two-photon coincidence counts with respect to a clock signal, used to center the JSI plots, in 24 hours. The clock consisted of a third SNSPD triggered by an independent PDC source pumped by the same laser (more details provided in the Supplemental Material [21], Sec. 3). We reconstruct the JSI over a 36 nm spectral range, ~ 12 times larger than the PDC photons' bandwidth, to ensure reliable estimation of the JSI properties [20]. The results are shown in Fig. 3(a). The overlay contours show the theoretical pump spectrum and the expected PMF (assuming the ideal crystal domain structure and a sech^2 pump function). There is excellent correspondence between the

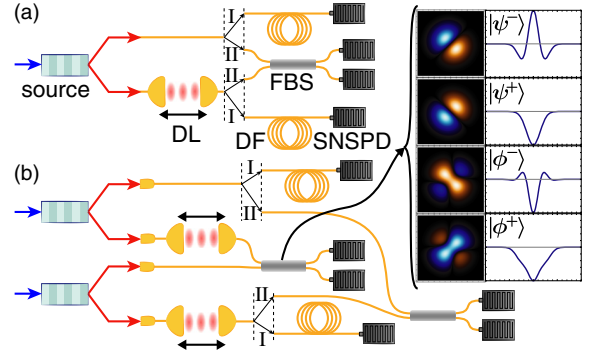


FIG. 2. Experimental setup. (a) Biphoton state characterization: joint-spectrum reconstruction via dispersive fiber (DF) time-of-flight spectroscopy (modes I) and HOM interference in a fiber beam splitter (FBS) (modes II). (b) Entanglement swapping setup: successful entanglement swapping is heralded by a coincidence detection of the photons after the FBS. The swapped state is again verified via fiber spectroscopy (modes I) and HOM interference (modes II). We note that a setup similar to (modes I) has been used to investigate the spectral properties of HOM interference [30]. The panel on the right shows the four possible Bell-state projections at the BS, and the corresponding interference pattern.

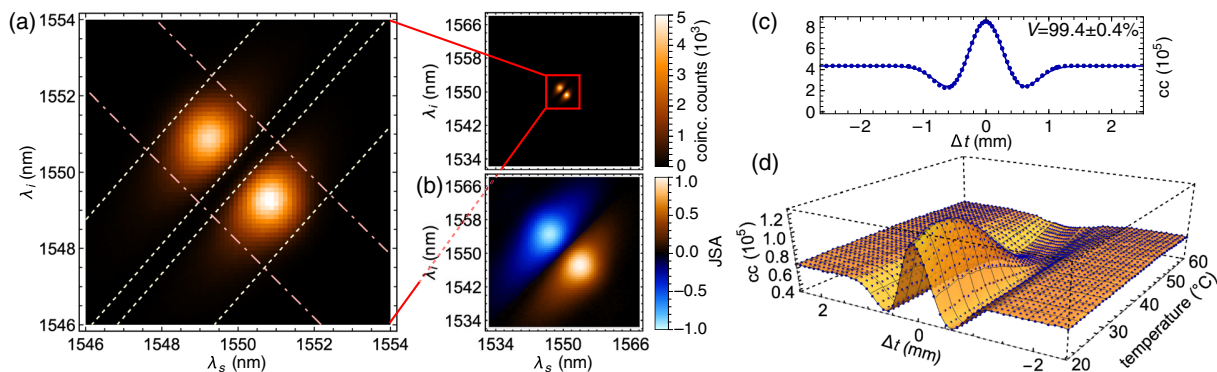


FIG. 3. Single source characterization. (a) Measured JSI (right) and zoom on a reduced, 8 nm spectral range (left) to show its main features. The bin size corresponds to 0.118 nm (see the Supplemental Material [21], Sec. 6 for details). The dot-dashed pink lines and yellow dashed lines are the $1/e^2$ contours of the sech^2 pump’s intensity, and of the PMF’s absolute value squared calculated from the crystal domain structure, respectively. (b) Reconstructed effective JSA. (c) Signal-idler interference pattern. (d) Signal-idler interference varying crystal temperature. The HOM visibility has a maximum at 25 degrees, while no antibunching occurs above 39 degrees. Error bars assuming Poissonian counting statistics are smaller than the symbol size.

theoretical target and the measured JSI, which faithfully reproduces not only the two main peaks but also the spectral bandwidth.

The HOM setup is shown in Fig. 2(a), modes II: the interference pattern is measured by delaying one photon with respect to the other before they interfere in a fiber BS. While two-photon interference is typically destructive and, for PDC photons, exhibits a characteristic triangular or Gaussian “dip” [19], antibunching at the BS can occur whenever the biphoton state is at least partially antisymmetric under particle exchange: more antisymmetry results in more antibunching [31] (see the Supplemental Material [21], Sec. 4 for proof). Remarkably, for a biphoton state that is separable in all other DOFs, antibunching corresponds to entanglement in the biphoton spectrum [32]. We use this result to verify TFM entanglement in our generated state. We show the experimental data in Fig. 3(c): the fitted HOM visibility is equal to $99.4 \pm 0.4\%$, certifying a high degree of spectral entanglement of the PDC biphoton state (the fitting function is given in the Supplemental Material [21], Sec. 1).

Finally, HOM interference between heralded PDC-photons generated by two identical sources can be used to estimate the Schmidt number of the biphoton state [19,33]: since the $|\psi^-\rangle$ state in Eq. (1) is composed of two equally weighted TFM basis states, the corresponding Schmidt number is expected to be equal to 2. We measure a HOM visibility of $48.8 \pm 1.2\%$ at 30 mW of average pump power (see the Supplemental Material [21], Sec. 5 for details), which corresponds to a Schmidt number of 2.05 ± 0.05 , in excellent agreement with theory.

While the JSI reconstruction doesn’t contain any phase information, we can exploit our knowledge of the antisymmetry and Schmidt number of the biphoton wave function to reconstruct an “effective” JSA. Specifically,

to guarantee antisymmetry and bimodal structure of the quantum state, we impose an $e^{i\pi}$ sign shift between the two peaks of the square root of the measured JSI. This antisymmetric phase shift matches, up to an additional linear phase, the output of the nonlinearity-engineering algorithm that generates the state in Eq. (1). The true JSA might instead have nonlinear phase terms, as long as they do not affect the Schmidt number we obtained from the heralded-photon HOM measurement (see the Supplemental Material [21], Sec. 5 for further discussion). The effective JSA obtained in this way is depicted in Fig. 3(b). It qualitatively matches the theoretical target JSA shown in Fig. 1(a) and has an effective Schmidt number of 2.026 ± 0.001 , consistent with the HOM measurement and with our numerical simulations (details on the JSI reconstruction and error estimation are discussed in the Supplemental Material [21], Sec. 6).

Small variations in the crystal domain widths can be introduced by changing the crystals temperature. This results in a shift of the PMF in the (ω_s, ω_i) plane, producing frequency nondegenerate photons and therefore compromising the antisymmetry of the biphoton wave function. Surprisingly, this doesn’t affect the Schmidt number of the quantum state: the biphoton state (1) remains intact, but the signal and idler TFMs are centered around different frequencies. This enables the capability of switching between an antisymmetric state to a nonantisymmetric one without spoiling the spectral modal structure. We observe the biphoton antisymmetry breaking by performing HOM scans at different temperatures, from 20 to 60 degrees at 1 degree intervals. We show the results in Fig. 3(d): antibunching (and therefore antisymmetry) is maximal for perfectly degenerate PDC and it reduces as we tune away from degeneracy, until no antibunching occurs above a certain center-frequency offset, as expected from theory.

Multiphoton protocols using TFMs will require the ability to interfere and swap independently generated TFM-encoded photons. While a generalized entanglement swapping for TFM has been proposed, it relies on a nonlinear process between two single photons and therefore has very low success probability [34]. Here we instead implement the standard entanglement swapping scheme with the setup shown in Fig. 2(b). Two entangled $|\psi^-\rangle$ states are produced via two independent engineered TFM-entangled pair sources. The overall four-photon state can be written as $1/2(|\phi^+\rangle|\phi^+\rangle + |\phi^-\rangle|\phi^-\rangle + |\psi^+\rangle|\psi^+\rangle - |\psi^-\rangle|\psi^-\rangle)$, a coherent sum of the four Bell states:

$$\begin{aligned} |\psi^\pm\rangle &= \frac{1}{\sqrt{2}} |\nearrow\rangle |\searrow\rangle \pm |\swarrow\rangle |\nwarrow\rangle \\ |\phi^\pm\rangle &= \frac{1}{\sqrt{2}} |\nearrow\rangle |\nearrow\rangle \pm |\searrow\rangle |\searrow\rangle. \end{aligned} \quad (2)$$

The joint spectra for all four Bell states and the corresponding HOM patterns are shown in the inset of Fig. 2(b): perfect antibunching at the BS occurs only for the singlet state, while triplet states bunch due to the symmetry of their wave functions. We use this to discern a successful projection on $|\psi^-\rangle$ from all the other outcomes: a two-photon coincidence detection at the two BS outputs corresponds to a projection on the singlet state and heralds swapping of the TFM $|\psi^-\rangle$ state from the two original photon pairs to the two non-interacting photons (see the Supplemental Material [21], Sec. 3 for details).

We benchmark the state obtained after entanglement swapping via fiber spectroscopy and HOM interference, as shown in Fig. 2(b), modes I and II, respectively. The JSI of the swapped $|\psi^-\rangle$ state is again measured by sending the two photons through a pair of 20 km fibers. In Fig. 4(a) we show the measured joint spectrum of the two-photon state without postselection heralded by either one or two detection events after the BS, corresponding to threefold and fourfold coincidence counts, respectively. We collect 670k threefold and ~ 46 k fourfold coincident counts in 72 hours of integration time. We observe four peaks, arising from a mixture of the four equally weighted Bell state JSAs [see Fig. 2(b)]. When we instead record fourfold coincident counts, we measure the spectrum of the swapped $|\psi^-\rangle$ biphoton state, recovering the two main peaks on the JSI's diagonal [Fig. 4(b)].

We then measure the HOM interference of the swapped state. Because the probability of generating photon pairs independently equals that of a double-pair emission in each source, the maximal theoretical HOM visibility is 25%—not a fundamental limitation, it only occurs when both photons of two PDC pairs are interfered, which is not required for, e.g., repeater protocols. We obtain a HOM visibility of $24.5 \pm 0.5\%$, as shown in Fig. 4(c). We subtract the multiphoton background determined through the detection of coincident counts when either of the two photon sources are blocked. The corrected interference pattern in Fig. 4(d) yields a HOM visibility of $97.1 \pm 1.7\%$,

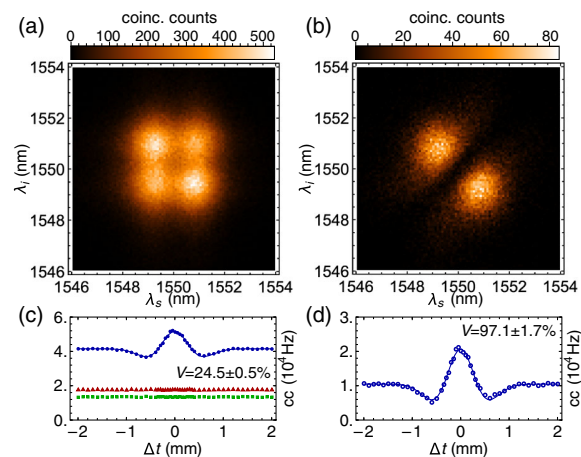


FIG. 4. Entanglement swapping results. (a) JSI reconstruction of the fully mixed state. The two peaks on the anti-diagonal have higher count rates because the contribution from the $|\psi^-\rangle$ state is counted twice in the threefold coincidences. (b) JSI reconstruction of the entanglement-swapped state. We display a 8 nm spectral range with 0.118 nm bin size to highlight the main JSI features. (c) HOM data without signal error correction. The blue data points are the fourfold coincidence counts detected by the SNSPDs when both the sources are active, while red triangles and green squares are the error signals measured by alternately blocking one of the two sources. (d) HOM data, corrected for higher-order emissions.

certifying success of the TFM entanglement swapping protocol.

We can now reconstruct the effective JSA of the swapped state under the assumptions discussed earlier, calculating a Schmidt number of 2.15 ± 0.01 —slightly higher than for the single-source scenario, as expected due to discrepancies between independent sources that affect the interference quality.

We have demonstrated the first instance of TFM entanglement generation enabled by nonlinearity engineering, achieving high generation rates, heralding efficiency and spectral entanglement. Due to its simplicity and quality, we expect this technique to be used in a host of different quantum information tasks. The flexibility in tailoring the PMF lends itself to the generation of high-dimensional TFM entanglement: not only can one use higher-order Hermite-Gaussian PMFs to upscale to qudits [10], but one can also aim at different PMF shapes for targeting specific applications, such as frequency multiplexing [35]. The same nonlinearity engineering technique can be used in asymmetric group-velocity matching condition [20] to generate pure, TFM-encoded single photons, as well as to implement mode filtering and TFM-projective measurements in a quantum pulse gate scheme, complementing the TFM framework based on pump spectral-shaping [5,10]. Finally, the ability to customize biphoton spectra could be useful for multiphoton quantum metrology applications in which measurement precision depends on the shape and steepness of the HOM pattern [36].

We thank J. Leach and M. Malik for loan of equipment, and D. Kundys and M. Proietti for useful discussions. This work was supported by the UK Engineering and Physical Sciences Research Council (Grant No. EP/N002962/1). F.G. acknowledges studentship funding from EPSRC under Grant No. EP/L015110/1. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

Note added.—Recently, a similar experiment has been reported [37] where TFM entanglement swapping is heralded by a frequency-resolved Bell-state measurement, and verified using a similar scheme.

*fraccalo@gmail.com

†These two authors contributed equally.

- [1] M. Erhard, M. Malik, M. Krenn, and A. Zeilinger, Experimental Greenberger-Horne-Zeilinger entanglement beyond qubits, *Nat. Photonics* **12**, 759 (2018).
- [2] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, Multidimensional quantum entanglement with large-scale integrated optics, *Science* **360**, 285 (2018).
- [3] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of Quantum Key Distribution Using d -Level Systems, *Phys. Rev. Lett.* **88**, 127902 (2002).
- [4] M. Huber and M. Pawłowski, Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement, *Phys. Rev. A* **88**, 032309 (2013).
- [5] B. Brecht, D. V. Reddy, C. Silberhorn, and M. G. Raymer, Photon Temporal Modes: A Complete Framework for Quantum Information Science, *Phys. Rev. X* **5**, 041017 (2015).
- [6] M. Kues, C. Reimer, P. Roztocky, L. R. Cortés, S. Sciara, B. Wetzel, Y. Zhang, A. Cino, S. T. Chu, B. E. Little, D. J. Moss, L. Caspani, J. Azaña, and R. Morandotti, On-chip generation of high-dimensional entangled quantum states and their coherent control, *Nature (London)* **546**, 622 (2017).
- [7] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, *Sci. Adv.* **3**, e1701491 (2017).
- [8] H.-H. Lu, J. M. Lukens, N. A. Peters, B. P. Williams, A. M. Weiner, and P. Lougovski, Quantum interference and correlation control of frequency-bin qubits, *Optica* **5**, 1455 (2018).
- [9] P. Imany, J. A. Jaramillo-Villegas, M. S. Alshaykh, J. M. Lukens, O. D. Odele, A. J. Moore, D. E. Leaird, M. Qi, and A. M. Weiner, High-dimensional optical quantum logic in large operational spaces, *npj Quantum Inf.* **5**, 59 (2019).
- [10] V. Ansari, J. M. Donohue, B. Brecht, and C. Silberhorn, Tailoring nonlinear processes for quantum optics with pulsed temporal-mode encodings, *Optica* **5**, 534 (2018).
- [11] Q. Ding, R. Chatterjee, Y. Huang, and T. Yu, High-dimensional temporal mode propagation in a turbulent environment, [arXiv:1907.02321](https://arxiv.org/abs/1907.02321).
- [12] A. Eckstein, B. Brecht, and C. Silberhorn, A quantum pulse gate based on spectrally engineered sum frequency generation, *Opt. Express* **19**, 13770 (2011).
- [13] A. Pe'er, B. Dayan, A. A. Friesem, and Y. Silberberg, Temporal Shaping of Entangled Photons, *Phys. Rev. Lett.* **94**, 073601 (2005).
- [14] N. Matsuda, Deterministic reshaping of single-photon spectra using cross-phase modulation, *Sci. Adv.* **2**, e1501223 (2016).
- [15] V. Averchenko, D. Sych, G. Schunk, U. Vogl, C. Marquardt, and G. Leuchs, Temporal shaping of single photons enabled by entanglement, *Phys. Rev. A* **96**, 043822 (2017).
- [16] C. J. McKinstrie, J. B. Christensen, K. Rottwitt, and M. G. Raymer, Generation of two-temporal-mode photon states by vector four-wave mixing, *Opt. Express* **25**, 20877 (2017).
- [17] S. Francesconi, F. Baboux, A. Raymond, N. Fabre, G. Boucher, A. Lemaître, P. Milman, M. Amanti, and S. Ducci, Engineering two-photon wavefunction and exchange statistics in a semiconductor chip, [arXiv:1907.07935](https://arxiv.org/abs/1907.07935).
- [18] F. Graffitti, D. Kundys, D. T. Reid, A. M. Brańczyk, and A. Fedrizzi, Pure down-conversion photons through sub-coherence-length domain engineering, *Quantum Sci. Technol.* **2**, 035001 (2017).
- [19] F. Graffitti, P. Barrow, M. Proietti, D. Kundys, and A. Fedrizzi, Independent high-purity photons created in domain-engineered crystals, *Optica* **5**, 514 (2018).
- [20] F. Graffitti, J. Kelly-Massicotte, A. Fedrizzi, and A. M. Brańczyk, Design considerations for high-purity heralded single-photon sources, *Phys. Rev. A* **98**, 053811 (2018).
- [21] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.124.053603> for additional details regarding experimental methods and extended theoretical derivations.
- [22] Y.-P. Huang and P. Kumar, Mode-resolved photon counting via cascaded quantum frequency conversion, *Opt. Lett.* **38**, 468 (2013).
- [23] V. Ansari, J. M. Donohue, M. Allgaier, L. Sansoni, B. Brecht, J. Roslund, N. Treps, G. Harder, and C. Silberhorn, Tomography and Purification of the Temporal-Mode Structure of Quantum Light, *Phys. Rev. Lett.* **120**, 213601 (2018).
- [24] D. V. Reddy and M. G. Raymer, High-selectivity quantum pulse gating of photonic temporal modes using all-optical Ramsey interferometry, *Optica* **5**, 423 (2018).
- [25] I. Jizan, B. Bell, L. G. Helt, A. C. Bedoya, C. Xiong, and B. J. Eggleton, Phase-sensitive tomography of the joint spectral amplitude of photon pair sources, *Opt. Lett.* **41**, 4803 (2016).
- [26] A. O. C. Davis, V. Thiel, and B. J. Smith, Measuring the quantum state of a photon pair entangled in frequency and time, [arXiv:1809.03727](https://arxiv.org/abs/1809.03727).
- [27] I. Gianani, Robust spectral phase reconstruction of time-frequency entangled bi-photon states, *Phys. Rev. Research* **1**, 033165 (2019).
- [28] M. Avenhaus, A. Eckstein, P. J. Mosley, and C. Silberhorn, Fiber-assisted single-photon spectrograph, *Opt. Lett.* **34**, 2873 (2009).

- [29] C. K. Hong, Z. Y. Ou, and L. Mandel, Measurement of Subpicosecond Time Intervals between Two Photons by Interference, *Phys. Rev. Lett.* **59**, 2044 (1987).
- [30] R.-B. Jin, T. Gerrits, M. Fujiwara, R. Wakabayashi, T. Yamashita, S. Miki, H. Terai, R. Shimizu, M. Takeoka, and M. Sasaki, Spectrally resolved Hong-Ou-Mandel interference between independent photon sources, *Opt. Express* **23**, 28836 (2015).
- [31] A. Fedrizzi, T. Herbst, M. Aspelmeyer, M. Barbieri, T. Jennewein, and A. Zeilinger, Anti-symmetrization reveals hidden entanglement, *New J. Phys.* **11**, 103052 (2009).
- [32] T. Douce, A. Eckstein, S.P. Walborn, A.Z. Khoury, S. Ducci, A. Keller, T. Coudreau, and P. Milman, Direct measurement of the biphoton Wigner function through two-photon interference, *Sci. Rep.* **3**, 3530 (2013).
- [33] A. M. Brańczyk, Hong-Ou-Mandel interference, [arXiv:1711.00080](https://arxiv.org/abs/1711.00080).
- [34] D. L. P. Vitullo, M. G. Raymer, B. J. Smith, M. Karpiński, L. Mejling, and K. Rottwitt, Entanglement swapping for generation of heralded time-frequency-entangled photon pairs, *Phys. Rev. A* **98**, 023836 (2018).
- [35] T. Hiemstra, T. F. Parker, P. C. Humphreys, J. Tiedau, M. Beck, M. Karpiński, B. J. Smith, A. Eckstein, W. S. Kolthammer, and I. A. Walmsley, Pure single photons from scalable frequency multiplexing, [arXiv:1907.10355](https://arxiv.org/abs/1907.10355).
- [36] A. Lyons, G. C. Knee, E. Bolduc, T. Roger, J. Leach, E. M. Gauger, and D. Faccio, Attosecond-resolution Hong-Ou-Mandel interferometry, *Sci. Adv.* **4**, eaap9416 (2018).
- [37] S. Merkouche, V. Thiel, A. O. C. Davis, and B. J. Smith, Two-color Bell states heralded via entanglement swapping, [arXiv:1910.06506](https://arxiv.org/abs/1910.06506).

Direct generation of tailored pulse-mode entanglement - Supplemental Material

Francesco Graffitti,¹ Peter Barrow,¹ Alexander Pickston,¹ Agata M. Brańczyk,² and Alessandro Fedrizzi¹

¹*Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK*

²*Perimeter Institute for Theoretical Physics, Waterloo, Ontario, N2L 2Y5, Canada*

This document provides Supplemental Material to “Direct generation of tailored pulse-mode entanglement”. The document is structured as follows: In Section 1 we introduce the theoretical JSA and its components; In Section 2 we discuss the details of the nonlinearity engineering technique; In Section 3 we give more details on the experimental implementation of our scheme; In Section 4 we calculate the exact correspondence between the symmetry of the JSA and the interference visibility; In Section 5 we discuss the Schmidt number measurement and the effective JSA reconstruction; In Section 6 we give some details on the JSI reconstruction.

1. THEORETICAL JSA AND SPECTRAL MODES

The JSA in Fig. 1(a) of the main text is obtained by combining a Gaussian pump with an antisymmetric PMF shaped as the first order Hermite-Gaussian function multiplied by a Gaussian envelope:

$$\begin{aligned}\alpha(\omega_s, \omega_i) &= e^{-\frac{(\omega_s + \omega_i)^2}{2\sigma^2}} \\ \phi(\omega_s, \omega_i) &= e^{-\frac{(\omega_s - \omega_i)^2}{2\sigma^2}} (\omega_s - \omega_i).\end{aligned}\tag{S1}$$

The corresponding PDC first-order emission biphoton state reads:

$$\begin{aligned}|\psi^-(\omega_s, \omega_i)\rangle_{s,i} &= \iint d\omega_s d\omega_i \alpha(\omega_s, \omega_i) \phi(\omega_s, \omega_i) a_s^\dagger(\omega_s) a_i^\dagger(\omega_i) |0\rangle_{s,i} \\ &= \iint d\omega_s d\omega_i \exp\left[-\frac{\omega_s^2 + \omega_i^2}{\sigma^2}\right] (\omega_s - \omega_i) a_s^\dagger(\omega_s) a_i^\dagger(\omega_i) |0\rangle_{s,i},\end{aligned}\tag{S2}$$

where we are omitting the wavefunction normalisation. (S2) can be decomposed into the convex sum of a set of orthonormal one-variable function by performing the Schmidt decomposition:

$$\begin{aligned}|u(\omega_j)\rangle_j &\equiv |\wedge\rangle_j = \int d\omega_j \exp\left[-\frac{\omega_j^2}{\sigma^2}\right] a_j^\dagger(\omega_j) |0\rangle_j \\ |v(\omega_j)\rangle_j &\equiv |\vee\rangle_j = \int d\omega_j \exp\left[-\frac{\omega_j^2}{\sigma^2}\right] \omega_j a_j^\dagger(\omega_j) |0\rangle_j,\end{aligned}\tag{S3}$$

with $j = s, i$. The shape of the two spectral modes is shown in Fig. 1(a). Following from (S3), the biphoton state can be therefore written as follows:

$$\begin{aligned}|\psi^-(\omega_s, \omega_i)\rangle_{s,i} &= \frac{1}{\sqrt{2}} (|u(\omega_s)\rangle_s |v(\omega_i)\rangle_i - |v(\omega_s)\rangle_s |u(\omega_i)\rangle_i) \\ &= \frac{1}{\sqrt{2}} (|\wedge\rangle_s |\vee\rangle_i - |\vee\rangle_s |\wedge\rangle_i).\end{aligned}\tag{S4}$$

The state in (S4) is a maximally entangled singlet state in the spectral-temporal mode basis.

The expected HOM interference pattern corresponding to this state can be calculated as described in [1], and has the form:

$$p_{cc}(\Delta t) = \frac{1}{2} - \frac{1}{4} e^{-\frac{1}{4}\sigma^2 \Delta t^2} (\sigma^2 \Delta t^2 - 2),\tag{S5}$$

where p_{cc} is the coincidence-count probability after interference, σ depends on the biphoton bandwidth and Δt is the relative arrival time of the two photons at the BS. We use (S5) (with an additional visibility scaling factor) to fit the HOM data.

2. ENGINEERING ALGORITHM

We use the domain engineering technique introduced in [2] to shape the PMF of the crystal to an almost-arbitrary function. For generating the two-photon entangled state described in (S4), we need a PMF (Φ) of the form:

$$\Phi(\Delta k) = \exp \left[-\frac{\sigma^2}{2} (\Delta k - \Delta k_0)^2 \right] (\Delta k - \Delta k_0), \quad (\text{S6})$$

where σ is the parameter determining the PMF's width, Δk is the momentum mismatch, $\Delta k_0 = \pi/\ell$ is the quasi-phase-matching momentum, being ℓ the coherence length of the process (2ℓ corresponds to the poling period of a standard periodically poled crystal). An inverse Fourier transform of (S6) gives the target nonlinearity profile along the crystal:

$$g_{\text{target}}(x) = \mathcal{FT}^{-1} [\Phi(\Delta k)] = i \exp \left[-\frac{(x - \frac{L}{2})^2}{2\sigma^2} \right] \exp [i\Delta k_0 x] \left(x - \frac{L}{2} \right), \quad (\text{S7})$$

with L the crystal length, and where we have omitted the multiplicative constant. By integrating $g_{\text{target}}(x)$ along the longitudinal direction of the crystal, we obtain the target phase-matching function that our algorithm needs to track:

$$\begin{aligned} \Phi_{\text{target}}(x, \Delta k = \Delta k_0) &= -i \int_0^x g_{\text{target}}(x') e^{i\Delta k x'} dx' \Big|_{\Delta k_0} = \\ &= -i \frac{2\sqrt{e}}{\pi\sigma} \exp \left[-\frac{L^2 + 4x^2}{8\sigma^2} \right] \left(\exp \left[\frac{x^2}{2\sigma^2} \right] - \exp \left[\frac{Lx}{2\sigma^2} \right] \right) \sigma^2, \end{aligned} \quad (\text{S8})$$

where the prefactor is chosen for matching the maximum function's slope allowed by the field tracking algorithm in order to maximise the photon pairs production [2]. The parameters chosen for this experiment are $L = 30\text{mm}$ and $\sigma = L/5$. Fig. 1(b) in the main text shows the tracking function described in (S8) and the corresponding overall phase-matching function along the crystal.

3. EXPERIMENTAL SCHEME

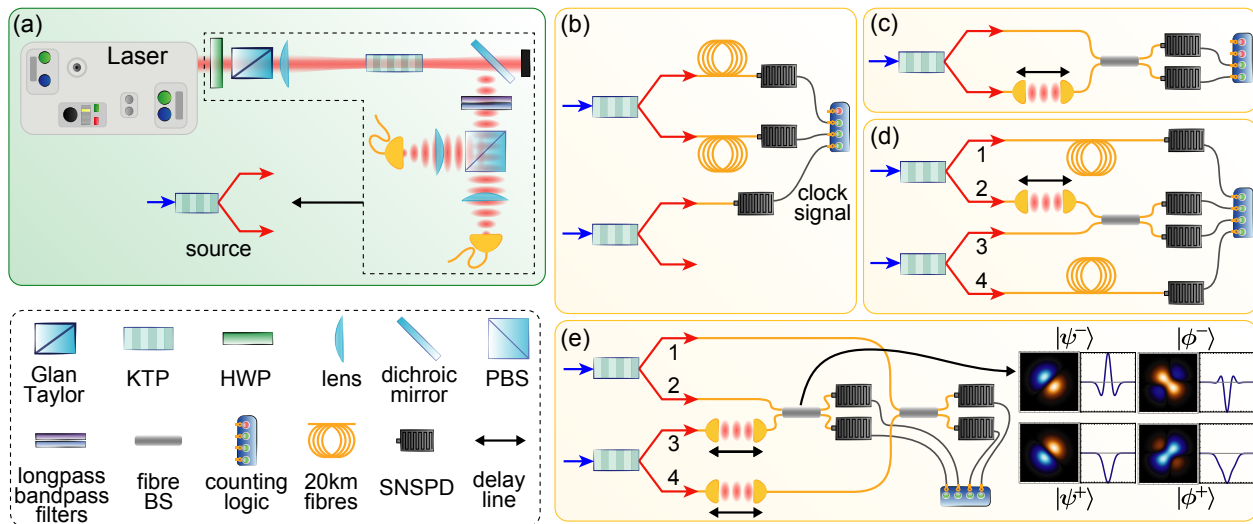


FIG. S1. Experimental setup. (a), Collinear PDC source. (b) Signal-idler JSI reconstruction. (c) Signal-idler HOM setup. (d) JSI reconstruction of the entanglement swapped state. (e) Entanglement swapping HOM setup.

The TFM entangled photon source consists in the collinear PDC source shown in Fig. S1(a). A 80 MHz, pulsed Ti:Sapphire laser (*Spectra-Physics: Tsunami*) is filtered in polarisation by a Glan-Taylor polariser, and focused into the nonlinearity-engineered KTP crystal. Pairs of orthogonally-polarised photon are produced in a collinear, type-II

downconversion process. The 1550 nm photons are filtered from the 775 nm pump pulse with a dichroic mirror and a longpass filter, and are then loosely filtered with a bandpass filter (~ 3 times broader than the PDC photons' bandwidth) to remove any additional spectral noise. A polarising beamsplitter separates signal and idler before they are coupled into single-mode fibres.

Fig. S1(b) shows the signal-idler JSI reconstruction setup. Each PDC photon is sent through a ~ 20 km single-mode fibre to convert spectral to temporal information exploiting the fibre dispersion of ~ 18 ps/km/nm at 1550 nm. The arrival time of the PDC photons is measured with respect to a clock signal provided by the detection (via a third SNSPD) of single-photons generated by an additional PDC source synchronously pumped by the same laser pulse that also pumps the PDC source. Such clock signal has < 50 ps timing jitter (corresponding to the detector jitter) and ~ 0.9 MHz rate.

Fig. S1(d,e) show the entanglement swapping setup. The four-photons state produced by the two PDC sources is $|\psi^-\rangle_{1,2}|\psi^-\rangle_{3,4}$, where the labels correspond to the modes 1, 2, 3, 4 shown in Fig. S1(d,e). This state can be rewritten considering a different bipartition of the Hilbert space:

$$\frac{1}{2}(|\phi^+\rangle_{2,3}|\phi^+\rangle_{1,4} + |\phi^-\rangle_{2,3}|\phi^-\rangle_{1,4} + |\psi^+\rangle_{2,3}|\psi^+\rangle_{1,4} - |\psi^-\rangle_{2,3}|\psi^-\rangle_{1,4}); \quad (\text{S9})$$

where the $|\dots\rangle_{2,3}$ states correspond to the photons interfering in the BS; the $|\dots\rangle_{1,4}$ state corresponds to the two non-interfering photons. Amongst the four possible Bell states in modes (2, 3), only the singlet $|\psi^-\rangle_{2,3}$ is antisymmetric and antibunches at the BS, exiting from opposite ports, while the other three triplet states bunch at the BS, exiting from the same port, as we show in the HOM patterns in Fig. S1(e). Whenever the counting logic detects two clicks of the SNSPDs at the BS outputs, a successful swapping of the $|\psi^-\rangle_{1,4}$ state on the non-interfering photons is heralded. Finally, the photons in modes (1, 4) are either sent in long fibres for the JSI reconstruction (Fig. S1(d)) or into a BS for the HOM interference (Fig. S1(e)): overall, only four-clicks events correspond to the heralding and measurement of the swapped state.

Unlike the standard biphoton JSI reconstruction we show in Fig. S1(b), where an external clock signal is needed to reference the arrival time of signal and idler, in our entanglement swapping scheme a two-clicks event in the SNSPDs at the output of the BS acts both as herald of a successful projection on $|\psi^-\rangle_{2,3}$, and as a clock signal for the arrival time of the photons in modes (1, 4). This is possible because the photons in modes (2, 3) after the BS are not sent through long fibres, and their arrival time is well defined in time (and within the detector jitter window): therefore, there is no need for an additional clock signal.

4. CORRESPONDENCE BETWEEN JSA ANTISYMMETRY AND INTERFERENCE ANTIBUNCHING

Any JSA can be decomposed in its symmetric and antisymmetric parts as follows:

$$\begin{aligned} f(\omega_s, \omega_i) &= \frac{f(\omega_s, \omega_i) + f(\omega_i, \omega_s)}{2} + \frac{f(\omega_s, \omega_i) - f(\omega_i, \omega_s)}{2} \\ f(\omega_s, \omega_i) &= \gamma f_s(\omega_s, \omega_i) + \delta f_a(\omega_s, \omega_i), \end{aligned} \quad (\text{S10})$$

where $f_s(\omega_s, \omega_i) = f_s(\omega_i, \omega_s)$, $f_a(\omega_s, \omega_i) = -f_a(\omega_i, \omega_s)$ are normalised functions:

$$\iint d\omega_s d\omega_i |f_s(\omega_s, \omega_i)|^2 = \iint d\omega_s d\omega_i |f_a(\omega_s, \omega_i)|^2 = 1, \quad (\text{S11})$$

and γ, δ need to satisfy the following condition: $|\gamma|^2 + |\delta|^2 = 1$.

The probability of having coincident counts after the BS (i.e. antibunching) reads [1]:

$$p_{\text{cc}}(\Delta t) = \frac{1}{2} - \frac{1}{2} \iint d\omega_s d\omega_i f^*(\omega_s, \omega_i) f(\omega_i, \omega_s) e^{i(\omega_i - \omega_s)\Delta t}. \quad (\text{S12})$$

We now replace the JSA with its decomposition in symmetric and antisymmetric parts, and consider the photons

arriving at the same time at the BS ($\Delta t = 0$):

$$p_{\text{cc}}(0) = \frac{1}{2} - \frac{1}{2} \iint d\omega_s d\omega_i \left(|\gamma|^2 |f_s(\omega_s, \omega_i)|^2 - \gamma^* \delta f_s^*(\omega_s, \omega_i) f_a(\omega_s, \omega_i) + \gamma \delta^* f_a^*(\omega_s, \omega_i) f_s(\omega_s, \omega_i) - |\delta|^2 |f_a(\omega_s, \omega_i)|^2 \right). \quad (\text{S13})$$

The integral of the mixed terms is equal to zero because the overall product of f_s and f_a is antisymmetric, and considering the normalisation conditions in (S11) the coincidence probability reads:

$$p_{\text{cc}}(0) = \frac{1}{2} - \frac{1}{2} (|\gamma|^2 - |\delta|^2) = 1 - |\gamma|^2 = |\delta|^2. \quad (\text{S14})$$

5. SCHMIDT NUMBER ESTIMATION AND EFFECTIVE JSA RECONSTRUCTION

The spectral purity (and, consequently, the Schmidt number) of the JSA can be mapped to the interference visibility in an heralded-photon HOM experiment between two identical PDC sources [1, 3]. This can be measured with a setup analogous to Fig. S1(e), without one of the two HOM interference stages (i.e. only one photon from each source is interfered in the BS, while the other is sent to an SNSPD and used for heralding). With such scheme, we measure a HOM visibility of $48.8 \pm 1.2\%$ at 30 mW of average pump power (see Fig. S2 for the data), which corresponds to a Schmidt number of 2.05 ± 0.05 , in excellent agreement with the Schmidt number 2 expected for the maximally antisymmetric singlet state.

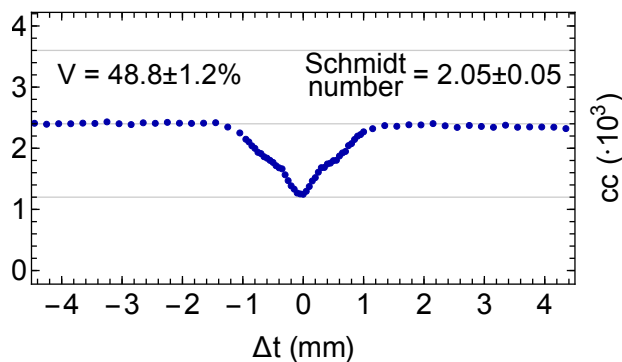


FIG. S2. Heralded HOM interference data.

The JSI reconstruction provides full information on the absolute value of the JSA, but it doesn't give any information on the phase of the biphoton state. In the case of Eq. (S2), the value of $|JSA|$ corresponds to:

$$|f(\omega_s, \omega_i)| = \exp \left[-\frac{\omega_s^2 + \omega_i^2}{\sigma^2} \right] |\omega_s - \omega_i|, \quad (\text{S15})$$

which is in good agreement with the JSI we measured and showed in Fig. 3 of the main text. Any additional phase that multiplies Eq. (S15) has to provide an antisymmetric state in the signal and idler frequencies, otherwise it wouldn't produce a HOM peak: moreover, it also has to preserve the very specific interference pattern we derived in Eq. (S5) and measured with the setup in Fig. S1(c). In particular, we restrict our analysis on JSA phase to a function of the form $(\omega_s - \omega_i)$: this is a good approximation for the symmetric group velocity matching condition, where the dependence of Δk on the signal and idler frequencies rising from the phase-matching function is linear and perpendicular to the pump field [4].

We now consider a π phase between the two JSA peaks and an additional linear phase: this is the expected PMF structure produced by the nonlinearity engineering scheme used to design the crystal, as shown in Fig. S3. Under this assumption, the JSA reads:

$$f(\omega_s, \omega_i) = \exp \left[-\frac{\omega_s^2 + \omega_i^2}{\sigma^2} \right] (\omega_s - \omega_i) \exp [i \text{const} (\omega_s - \omega_i)], \quad (\text{S16})$$

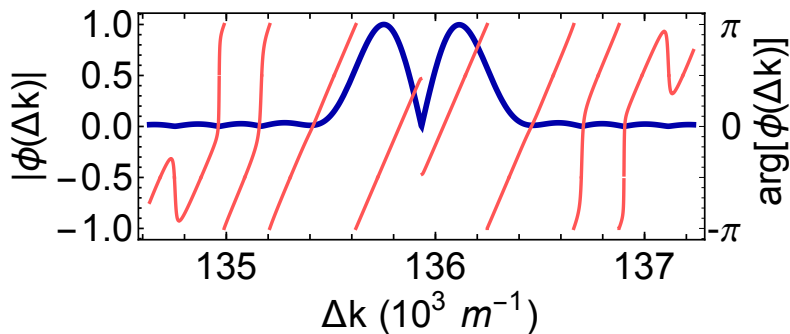


FIG. S3. Absolute value of the PMF (blue line) and corresponding phase (red line). The phase is linear (except in regions where the amplitude is almost zero), and has a π phase shift between the two peaks.

where “const” is the gradient of the phase, and the Schmidt decomposition provides the corresponding orthonormal modes:

$$\begin{aligned}
 |u(\omega_j)\rangle_j &\equiv |\wedge\rangle_j = \int d\omega_j \exp\left[-\frac{\omega_j^2}{\sigma^2} \pm i \text{const } \omega_j\right] a_j^\dagger(\omega_j) |0\rangle_j \\
 |v(\omega_j)\rangle_j &\equiv |\vee\rangle_j = \int d\omega_j \exp\left[-\frac{\omega_j^2}{\sigma^2} \pm i \text{const } \omega_j\right] \omega_j a_j^\dagger(\omega_j) |0\rangle_j,
 \end{aligned}
 \tag{S17}$$

where the $+$ ($-$) sign is used for the signal (idler) photon. The Schmidt number corresponding to Eq. (S17) is 2, as for the antisymmetric JSA without linear phase in Eq. (S2), and the overall JSA is still antisymmetric. The corresponding HOM pattern reads:

$$p_{cc}(\Delta t) = \frac{1}{2} - \frac{1}{4} e^{-\frac{1}{4}\sigma^2(\Delta t + 2\text{const})^2} (\sigma^2(\Delta t + 2\text{const})^2 - 2),
 \tag{S18}$$

which still exhibits perfect antibunching and the same shape. This phase is therefore a suitable candidate for describing the measured quantum state, as expected from the crystal engineering technique used to tailor the PMF and consequently the JSA of the PDC process. Other phase structures might, in principle, give rise to a JSA having a Schmidt number equal to 2 while preserving the same HOM structure: testing this possibility would require a phase-sensitive JSA reconstruction [5–7].

6. JSI RECONSTRUCTION AND ERROR ESTIMATION

The measured JSIs are 12250×12250 matrices, where each bin has a size of 1×1 ps, corresponding to the timing logic’s resolution. We calibrate our dispersive-fibre spectrometer with a reference signal with respect to a commercial single-photon CCD spectrometer, obtaining a scaling factor of ~ 2.94 pm/ps (centred around 1550 nm). This corresponds to a total measurement spectral range of ~ 36 nm. We down-sample the JSIs to 40×40 ps bins for reducing the sparsity of the data and computing the singular value decomposition (as numerical implementation of the Schmidt decomposition). The error on the extracted Schmidt numbers represents 3σ statistical confidence regions obtained via Monte-Carlo re-sampling (10k runs of the algorithm) assuming a Poissonian statistics on the coincident counts distribution.

-
- [1] A. M. Brańczyk, Hong-Ou-Mandel interference, arXiv (2017), [arXiv:1711.00080](https://arxiv.org/abs/1711.00080).
 - [2] F. Graffitti, D. Kundys, D. T. Reid, A. M. Brańczyk, and A. Fedrizzi, Pure down-conversion photons through sub-coherence-length domain engineering, *Quantum Science and Technology* **2**, 035001 (2017).
 - [3] F. Graffitti, P. Barrow, M. Proietti, D. Kundys, and A. Fedrizzi, Independent high-purity photons created in domain-engineered crystals, *Optica* **5**, 514 (2018).

- [4] F. Graffitti, J. Kelly-Massicotte, A. Fedrizzi, and A. M. Brańczyk, Design considerations for high-purity heralded single-photon sources, *Phys. Rev. A* **98**, 053811 (2018).
- [5] I. Jizan, B. Bell, L. G. Helt, A. C. Bedoya, C. Xiong, and B. J. Eggleton, Phase-sensitive tomography of the joint spectral amplitude of photon pair sources, *Opt. Lett.* **41**, 4803 (2016).
- [6] A. O. C. Davis, V. Thiel, and B. J. Smith, Measuring the quantum state of a photon pair entangled in frequency and time, *arXiv* (2018), [arXiv:1809.03727](https://arxiv.org/abs/1809.03727).
- [7] I. Gianani, Robust spectral phase reconstruction of time-frequency entangled bi-photon states, *Phys. Rev. Research* **1**, 033165 (2019).

Bibliography

- [1] A. Einstein, B. Podolsky, and N. Rosen. “Can quantum-mechanical description of physical reality be considered complete?” *Physical Review*, volume 47(10):777–780, 1935. doi:10.1103/PhysRev.47.777.
- [2] J. S. Bell. “On the Einstein Podolsky Rosen paradox”. *Physics Physique Fizika*, volume 1(3):195–200, 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.
- [3] G. Brassard. “Brief history of quantum cryptography: a personal perspective”. In “IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.”, pages 19–23. 2005. doi:10.1109/ITWTPI.2005.1543949.
- [4] S. Wiesner. “Conjugate coding”. *ACM SIGACT News*, volume 15(1):78–88, 1983. doi:10.1145/1008908.1008920.
- [5] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. “Quantum Cryptography, or Unforgeable Subway Tokens”. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, “Advances in Cryptology”, pages 267–275. Springer US, Boston, MA, 1983. doi:10.1007/978-1-4757-0602-4_26.
- [6] C. H. Bennett and G. Brassard. “An Update on Quantum Cryptography”. In G. R. Blakley and D. Chaum, editors, “Advances in Cryptology”, volume 196, pages 475–480. Springer Berlin Heidelberg, Berlin, Heidelberg, 1985. doi:10.1007/3-540-39568-7_39.
- [7] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. *Theoretical Computer Science*, volume 560:7–11, 2014. doi:10.1016/j.tcs.2014.05.025.
- [8] R. P. Feynman. “Simulating physics with computers”. *International Journal of Theoretical Physics*, volume 21(6):467–488, 1982. doi:10.1007/BF02650179.
- [9] P. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In “Proceedings 35th Annual Symposium on Foundations of Computer Science”, pages 124–134. 1994. doi:10.1109/SFCS.1994.365700.
- [10] L. K. Grover. “A fast quantum mechanical algorithm for database search”. *arXiv:quant-ph/9605043*, 1996. ArXiv: quant-ph/9605043.
- [11] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”. *Physical Review Letters*, volume 70(13):1895–1899, 1993. doi:10.1103/PhysRevLett.70.1895.

- [12] D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. “Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels”. *Physical Review Letters*, volume 80(6), 1998. doi:10.1103/PhysRevLett.80.1121.
- [13] M. Żukowski. “Bell theorem involving all settings of measuring apparatus”. *Physics Letters A*, volume 177(4):290–296, 1993. doi:10.1016/0375-9601(93)90002-H.
- [14] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. “Experimental entanglement Swapping: Entangling photons that never interacted”. *Physical Review Letters*, volume 80(18), 1998. doi:10.1103/PhysRevLett.80.3891.
- [15] S. L. Braunstein, A. Mann, and M. Revzen. “Maximal violation of Bell inequalities for mixed states”. *Physical Review Letters*, volume 68(22), 1992. doi:10.1103/PhysRevLett.68.3259.
- [16] S. L. Braunstein and A. Mann. “Measurement of the Bell operator and quantum teleportation”. *Physical Review A*, volume 51(3), 1995. doi:10.1103/PhysRevA.51.R1727.
- [17] C. K. Hong, Z. Y. Ou, and L. Mandel. “Measurement of subpicosecond time intervals between two photons by interference”. *Physical Review Letters*, volume 59(18):2044–2046, 1987. doi:10.1103/PhysRevLett.59.2044.
- [18] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, *et al.* “Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres”. *Nature*, volume 526(7575):682–686, 2015. doi:10.1038/nature15759.
- [19] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White. “Photonic boson sampling in a tunable circuit”. *Science*, volume 339(6121):794–798, 2013. doi:10.1126/science.1231440.
- [20] H. Wang, J. Qin, X. Ding, M.-C. Chen, S. Chen, X. You, Y.-M. He, X. Jiang, L. You, *et al.* “Boson sampling with 20 input photons and a 60-mode interferometer in a 10^{14} -dimensional hilbert space”. *Physical Review Letters*, volume 123(25):250503, 2019. doi:10.1103/PhysRevLett.123.250503.
- [21] D. N. Klyshko. “The effect of focusing on photon correlation in parametric light scattering”. *Zhurnal Eksperimentalnoi i Teoreticheskoi Fiziki*, volume 94:82–90, 1988.
- [22] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, *et al.* “Experimental quantum repeater without quantum memory”. *Nature Photonics*, volume 13(9):644–648, 2019. doi:10.1038/s41566-019-0468-5.
- [23] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih. “New high-intensity source of polarization-entangled photon pairs”. *Physical Review Letters*, volume 75(24):4337–4341, 1995. doi:10.1103/PhysRevLett.75.4337.

- [24] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling. “Entangled photon-pair sources based on three-wave mixing in bulk crystals”. *Review of Scientific Instruments*, volume 92(4):041101, 2021. doi:10.1063/5.0023103.
- [25] M. Krenn, M. Malik, M. Erhard, and A. Zeilinger. “Orbital angular momentum of photons and the entanglement of Laguerre–Gaussian modes”. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, volume 375(2087), 2017. doi:10.1098/rsta.2015.0442.
- [26] A. Forbes and I. Nape. “Quantum mechanics with patterns of light: Progress in high dimensional and multidimensional entanglement with structured light”. *AVS Quantum Science*, volume 1(1), 2019. doi:10.1116/1.5112027.
- [27] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. “Pulsed energy-time entangled twin-photon source for quantum communication”. *Physical Review Letters*, volume 82(12), 1999. doi:10.1103/PhysRevLett.82.2594.
- [28] M. Avenhaus, M. V. Chekhova, L. A. Krivitsky, G. Leuchs, and C. Silberhorn. “Experimental verification of high spectral entanglement for pulsed waveguided spontaneous parametric down-conversion”. *Physical Review A*, volume 79(4):043836, 2009. doi:10.1103/PhysRevA.79.043836.
- [29] M. Fujiwara, M. Toyoshima, M. Sasaki, K. Yoshino, Y. Nambu, and A. Tomita. “Performance of hybrid entanglement photon pair source for quantum key distribution”. *Applied Physics Letters*, volume 95(26), 2009. doi:10.1063/1.3276559.
- [30] X.-s. Ma, A. Qarry, J. Kofler, T. Jennewein, and A. Zeilinger. “Experimental violation of a Bell inequality with two different degrees of freedom of entangled particle pairs”. *Physical Review A*, volume 79(4), 2009. doi:10.1103/PhysRevA.79.042101.
- [31] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan. “Observation of eight-photon entanglement”. *Nature Photonics*, volume 6(4):225–228, 2012. doi:10.1038/nphoton.2011.354.
- [32] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, *et al.* “Experimental ten-photon entanglement”. *Physical Review Letters*, volume 117(21):210502, 2016. doi:10.1103/PhysRevLett.117.210502.
- [33] H.-S. Zhong, Y. Li, W. Li, L.-C. Peng, Z.-E. Su, Y. Hu, Y.-M. He, X. Ding, W. Zhang, *et al.* “12-photon entanglement and scalable scatter-shot boson sampling with optimal entangled-photon pairs from parametric down-conversion”. *Physical Review Letters*, volume 121(25):250505, 2018. doi:10.1103/PhysRevLett.121.250505.
- [34] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, *et al.* “Quantum computational advantage using photons”. *Science*, volume 370(6523):1460–1463, 2020. doi:10.1126/science.abe8770.
- [35] J. Preskill. “Quantum Computing in the NISQ era and beyond”. *Quantum*, volume 2, 2018. doi:10.22331/q-2018-08-06-79.

- [36] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, *et al.* “Quantum supremacy using a programmable superconducting processor”. *Nature*, volume 574(7779):505–510, 2019. doi:10.1038/s41586-019-1666-5.
- [37] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin. “Fault tolerant quantum computation with nondeterministic gates”. *Physical Review Letters*, volume 105(25):250502, 2010. doi:10.1103/PhysRevLett.105.250502.
- [38] E. Meyer-Scott, N. Montaut, J. Tiedau, L. Sansoni, H. Herrmann, T. J. Bartley, and C. Silberhorn. “Limits on the heralding efficiencies and spectral purities of spectrally filtered single photons from photon-pair sources”. *Physical Review A*, volume 95(6):061803, 2017. doi:10.1103/PhysRevA.95.061803.
- [39] T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, H. Zhou, J. Wang, Y. Liu, L.-K. Chen, *et al.* “Implementation of a 46-node quantum metropolitan area network”. *npj Quantum Information*, volume 7(1):1–6, 2021. doi:10.1038/s41534-021-00474-3.
- [40] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, *et al.* “An integrated space-to-ground quantum communication network over 4,600 kilometres”. *Nature*, volume 589(7841):214–219, 2021. doi:10.1038/s41586-020-03093-8.
- [41] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, *et al.* “Metropolitan all-pass and inter-city quantum communication network”. *Optics Express*, volume 18(26):27217–27225, 2010. doi:10.1364/OE.18.027217.
- [42] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, *et al.* “Field test of quantum key distribution in the tokyo QKD network”. *Optics Express*, volume 19(11):10387–10409, 2011. doi:10.1364/OE.19.010387.
- [43] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, *et al.* “Field test of wavelength-saving quantum key distribution network”. *Optics Letters*, volume 35(14):2454–2456, 2010. doi:10.1364/OL.35.002454.
- [44] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, *et al.* “Long-term performance of the SwissQuantum quantum key distribution network in a field environment”. *New Journal of Physics*, volume 13(12):123001, 2011. doi:10.1088/1367-2630/13/12/123001.
- [45] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, *et al.* “The SECOQC quantum key distribution network in vienna”. *New Journal of Physics*, volume 11(7):075001, 2009. doi:10.1088/1367-2630/11/7/075001.
- [46] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh. “Current status of the DARPA quantum network”. *arXiv:quant-ph/0503058*, 2005.
- [47] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge university press, Cambridge, 10th anniversary edition edition, 2010.

- [48] P. Kok and B. W. Lovett. *Introduction to Optical Quantum Information Processing*. Cambridge University Press, Cambridge, 2010. doi:10.1017/CBO9781139193658.
- [49] K. Fujii. *Quantum Computation with Topological Codes: From Qubit to Topological Fault-Tolerance*. SpringerBriefs in Mathematical Physics. Springer Singapore, 2015. doi:10.1007/978-981-287-996-7.
- [50] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski. “Multiphoton entanglement and interferometry”. *Reviews of Modern Physics*, volume 84(2), 2012. doi:10.1103/RevModPhys.84.777.
- [51] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. “Linear optical quantum computing with photonic qubits”. *Reviews of Modern Physics*, volume 79(1), 2007. doi:10.1103/RevModPhys.79.135.
- [52] D. Gottesman. “Class of quantum error-correcting codes saturating the quantum hamming bound”. *Physical Review A*, volume 54(3):1862–1868, 1996. doi:10.1103/PhysRevA.54.1862.
- [53] S. Aaronson and D. Gottesman. “Improved simulation of stabilizer circuits”. *Physical Review A*, volume 70(5):052328, 2004. doi:10.1103/PhysRevA.70.052328.
- [54] M. Van den Nest, J. Dehaene, and B. De Moor. “Graphical description of the action of local clifford transformations on graph states”. *Physical Review A*, volume 69(2):022316, 2021. doi:10.1103/PhysRevA.69.022316.
- [55] M. Hein, J. Eisert, and H. J. Briegel. “Multipartite entanglement in graph states”. *Physical Review A*, volume 69(6):062311, 2004. doi:10.1103/PhysRevA.69.062311.
- [56] Z. Ji, J. Chen, Z. Wei, and M. Ying. “The LU-LC conjecture is false”. *Quantum Information & Computation*, volume 10(1):97–108, 2010.
- [57] J. C. Adcock, S. Morley-Short, A. Dahlberg, and J. W. Silverstone. “Mapping graph state orbits under local complementation”. *Quantum*, volume 4:305, 2020. doi:10.22331/q-2020-08-07-305.
- [58] IBM. “Qiskit: An open-source framework for quantum computing”, 2021. doi:10.5281/zenodo.2573505.
- [59] A. M. Brańczyk. “Hong-ou-mandel interference”. *arXiv:1711.00080 [quant-ph]*, 2017.
- [60] G. Grynberg, A. Aspect, and C. Fabre. *Introduction to Quantum Optics: From the Semi-classical Approach to Quantized Light*. Cambridge University Press, Cambridge, 2010. doi:10.1017/CBO9780511778261.
- [61] R. W. Boyd. *Nonlinear optics*. Academic Press, Amsterdam ; Boston, 3rd ed edition, 2008.
- [62] R. Loudon. *The quantum theory of light*. Oxford science publications. Oxford University Press, Oxford ; New York, 3rd ed edition, 2000.

- [63] N. Quesada and J. E. Sipe. “Effects of time ordering in quantum nonlinear optics”. *Physical Review A*, volume 90(6), 2014. doi:10.1103/PhysRevA.90.063840.
- [64] N. Quesada and J. Sipe. “Time-ordering effects in the generation of entangled photons using nonlinear optical processes”. *Physical Review Letters*, volume 114(9), 2015. doi:10.1103/PhysRevLett.114.093903.
- [65] A. Christ, B. Brecht, W. Maurer, and C. Silberhorn. “Theory of quantum frequency conversion and type-II parametric down-conversion in the high-gain regime”. *New Journal of Physics*, volume 15(5), 2013. doi:10.1088/1367-2630/15/5/053038.
- [66] W. Sellmeier. “Ueber die durch die Aetherschwingungen erregten Mitschwingungen der Körpertheilchen und deren Rückwirkung auf die ersteren, besonders zur Erklärung der Dispersion und ihrer Anomalien”. 1872. doi:10.1002/andp.18722231105.
- [67] K. Kato and E. Takaoka. “Sellmeier and thermo-optic dispersion formulas for KTP”. *Applied Optics*, volume 41(24):5040, 2002. doi:10.1364/AO.41.005040.
- [68] S. Emanuelli and A. Arie. “Temperature-dependent dispersion equations for KTiOPO4 and KTiOAsO4”. *Applied Optics*, volume 42(33):6661, 2003. doi:10.1364/AO.42.006661.
- [69] F. Graffitti, J. Kelly-Massicotte, A. Fedrizzi, and A. M. Brańczyk. “Design considerations for high-purity heralded single-photon sources”. *Physical Review A*, volume 98(5):053811, 2018. doi:10.1103/PhysRevA.98.053811.
- [70] F. Laudenbach, S. Kalista, M. Hentschel, P. Walther, and H. Hübel. “A novel single-crystal & single-pass source for polarisation- and colour-entangled photon pairs”. *Scientific Reports*, volume 7(1), 2017. doi:10.1038/s41598-017-07781-w.
- [71] A. B. U’Ren, C. Silberhorn, R. Erdmann, K. Banaszek, W. P. Grice, I. A. Walmsley, and M. G. Raymer. “Generation of pure-state single-photon wavepackets by conditional preparation based on spontaneous parametric downconversion”. *arXiv:quant-ph/0611019*, 2006.
- [72] W. P. Grice, A. B. U’Ren, and I. A. Walmsley. “Eliminating frequency and space-time correlations in multiphoton states”. *Physical Review A*, volume 64(6), 2001. doi:10.1103/PhysRevA.64.063815.
- [73] P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. U’Ren, C. Silberhorn, and I. A. Walmsley. “Heralded generation of ultrafast single photons in pure quantum states”. *Physical Review Letters*, volume 100(13), 2008. doi:10.1103/PhysRevLett.100.133601.
- [74] C. K. Law, I. A. Walmsley, and J. H. Eberly. “Continuous frequency entanglement: Effective finite Hilbert space and entropy control”. *Physical Review Letters*, volume 84(23), 2000. doi:10.1103/PhysRevLett.84.5304.

- [75] M. Takeoka, R.-B. Jin, and M. Sasaki. “Full analysis of multi-photon pair effects in spontaneous parametric down conversion based photonic quantum information processing”. *New Journal of Physics*, volume 17(4), 2015. doi:10.1088/1367-2630/17/4/043030.
- [76] R.-B. Jin. “Efficient detection of an ultra-bright single-photon source using superconducting nanowire single-photon detectors”. *Optics Communications*, page 8, 2015.
- [77] P. A. Franken and J. F. Ward. “Optical harmonics and nonlinear phenomena”. *Reviews of Modern Physics*, volume 35(1):23–39, 1963. doi:10.1103/RevModPhys.35.23.
- [78] J. A. Armstrong, N. Bloembergen, J. Ducuing, and P. S. Pershan. “Interactions between light waves in a nonlinear dielectric”. *Physical Review*, volume 127(6):1918–1939, 1962. doi:10.1103/PhysRev.127.1918.
- [79] M. Fejer, G. Magel, D. Jundt, and R. Byer. “Quasi-phase-matched second harmonic generation: tuning and tolerances”. *IEEE Journal of Quantum Electronics*, volume 28(11):2631–2654, 1992. doi:10.1109/3.161322.
- [80] F. Graffitti. *Tailored quantum light for photonic quantum technologies.pdf*. Ph.D. thesis.
- [81] . Kornaszewski, M. Kohler, U. K. Sapaev, and D. T. Reid. “Designer femtosecond pulse shaping using grating-engineered quasi-phase-matching in lithium niobate”. *Optics Letters*, volume 33(4):378–380, 2008. doi:10.1364/OL.33.000378.
- [82] M. A. Arbore, A. Galvanauskas, D. Harter, M. H. Chou, and M. M. Fejer. “Engineerable compression of ultrashort pulses by use of second-harmonic generation in chirped-period-poled lithium niobate”. *Optics Letters*, volume 22(17):1341–1343, 1997. doi:10.1364/OL.22.001341.
- [83] G. Imeshev, A. Galvanauskas, D. Harter, M. A. Arbore, M. Proctor, and M. M. Fejer. “Engineerable femtosecond pulse shaping by second-harmonic generation with fourier synthetic quasi-phase-matching gratings”. *Optics Letters*, volume 23(11):864–866, 1998. doi:10.1364/OL.23.000864.
- [84] A. M. Brańczyk, A. Fedrizzi, T. M. Stace, T. C. Ralph, and A. G. White. “Engineered optical nonlinearity for quantum light sources”. *Optics Express*, volume 19(1):55–65, 2011. doi:10.1364/OE.19.000055.
- [85] C. Chen, J. E. Heyes, K.-H. Hong, M. Y. Niu, A. E. Lita, T. Gerrits, S. W. Nam, J. H. Shapiro, and F. N. C. Wong. “Indistinguishable single-mode photons from spectrally engineered biphotons”. *Optics Express*, volume 27(8):11626–11634, 2019. doi:10.1364/OE.27.011626.
- [86] C. Cui, R. Arian, S. Guha, N. Peyghambarian, Q. Zhuang, and Z. Zhang. “Wave-function engineering for spectrally uncorrelated biphotons in the telecommunication band based on a machine-learning framework”. *Physical Review Applied*, volume 12(3):034059, 2019. doi:10.1103/PhysRevApplied.12.034059.

- [87] C. Chen, C. Bo, M. Y. Niu, F. Xu, Z. Zhang, J. H. Shapiro, and F. N. C. Wong. “Efficient generation and characterization of spectrally factorable biphotons”. *Optics Express*, volume 25(7):7300–7312, 2017. doi:10.1364/OE.25.007300.
- [88] P. B. Dixon, J. H. Shapiro, and F. N. C. Wong. “Spectral engineering by gaussian phase-matching for quantum photonics”. *Optics Express*, volume 21(5):5879–5890, 2013. doi:10.1364/OE.21.005879.
- [89] A. Dosseva, . Cincio, and A. M. Brańczyk. “Shaping the joint spectrum of down-converted photons through optimized custom poling”. *Physical Review A*, volume 93(1):013801, 2016. doi:10.1103/PhysRevA.93.013801.
- [90] F. Graffitti, P. Barrow, M. Proietti, D. Kundys, and A. Fedrizzi. “Independent high-purity photons created in domain-engineered crystals”. *Optica*, volume 5(5):514–517, 2018. doi:10.1364/OPTICA.5.000514.
- [91] J.-L. Tambasco, A. Boes, L. G. Helt, M. J. Steel, and A. Mitchell. “Domain engineering algorithm for practical and effective photon sources”. *Optics Express*, volume 24(17):19616–19626, 2016. doi:10.1364/OE.24.019616.
- [92] F. Graffitti, D. Kundys, D. T. Reid, A. M. Brańczyk, and A. Fedrizzi. “Pure down-conversion photons through sub-coherence-length domain engineering”. *Quantum Science and Technology*, volume 2(3):035001, 2017. doi:10.1088/2058-9565/aa78d4.
- [93] D. T. Reid. “Engineered quasi-phase-matching for second-harmonic generation”. *Journal of Optics A: Pure and Applied Optics*, volume 5(4):S97–S102. doi:10.1088/1464-4258/5/4/362.
- [94] F. Graffitti, P. Barrow, A. Pickston, A. M. Brańczyk, and A. Fedrizzi. “Direct generation of tailored pulse-mode entanglement”. *Physical Review Letters*, volume 124(5):053603, 2021. doi:10.1103/PhysRevLett.124.053603.
- [95] F. Graffitti, V. D’Ambrosio, M. Proietti, J. Ho, B. Piccirillo, C. de Liso, L. Marrucci, and A. Fedrizzi. “Hyperentanglement in structured quantum light”. *Physical Review Research*, volume 2(4):043350, 2020. doi:10.1103/PhysRevResearch.2.043350.
- [96] R. S. Bennink. “Optimal collinear gaussian beams for spontaneous parametric down-conversion”. *Physical Review A*, volume 81(5):053805, 2010. doi:10.1103/PhysRevA.81.053805.
- [97] P. B. Dixon, D. Rosenberg, V. Stelmakh, M. E. Grein, R. S. Bennink, E. A. Dauler, A. J. Kerman, R. J. Molnar, and F. N. C. Wong. “Heralding efficiency and correlated-mode coupling of near-IR fiber-coupled photon pairs”. *Physical Review A*, volume 90(4):043804, 2014. doi:10.1103/PhysRevA.90.043804.
- [98] S. Ramelow, A. Mech, M. Giustina, S. Gröblacher, W. Wieczorek, J. Beyer, A. Lita, B. Calkins, T. Gerrits, *et al.* “Highly efficient heralding of entangled single photons”. *Optics Express*, volume 21(6):6707–6717, 2013. doi:10.1364/OE.21.006707.

- [99] M. D. C. Pereira, F. E. Becerra, B. L. Glebov, J. Fan, S. W. Nam, and A. Migdall. “Demonstrating highly symmetric single-mode, single-photon heralding efficiency in spontaneous parametric downconversion”. *Optics Letters*, volume 38(10):1609–1611, 2013. doi:10.1364/OL.38.001609.
- [100] J.-L. Smirr, M. Deconinck, R. Frey, I. Agha, E. Diamanti, and I. Zaquine. “Optimal photon-pair single-mode coupling in narrow-band spontaneous parametric downconversion with arbitrary pump profile”. *JOSA B*, volume 30(2):288–301, 2013. doi:10.1364/JOSAB.30.000288.
- [101] A. Pickston, F. Graffitti, P. Barrow, C. L. Morrison, J. Ho, A. M. Brańczyk, and A. Fedrizzi. “Optimised domain-engineered crystals for pure telecom photon sources”. *Optics Express*, volume 29(5):6991–7002, 2021. doi:10.1364/OE.416843.
- [102] A. M. Brańczyk, T. C. Ralph, W. Helwig, and C. Silberhorn. “Optimized generation of heralded Fock states using parametric down-conversion”. *New Journal of Physics*, volume 12(6):063001, 2010. doi:10.1088/1367-2630/12/6/063001.
- [103] W. P. Grice, R. S. Bennink, D. S. Goodman, and A. T. Ryan. “Spatial entanglement and optimal single-mode coupling”. *Physical Review A*, volume 83(2):023810, 2011. doi:10.1103/PhysRevA.83.023810.
- [104] M. Avenhaus, A. Eckstein, P. J. Mosley, and C. Silberhorn. “Fiber-assisted single-photon spectrograph”. *Optics Letters*, volume 34(18):2873–2875, 2009. doi:10.1364/OL.34.002873.
- [105] I. Jizan, B. Bell, L. G. Helt, A. C. Bedoya, C. Xiong, and B. J. Eggleton. “Phase-sensitive tomography of the joint spectral amplitude of photon pair sources”. *Optics Letters*, volume 41(20):4803–4806, 2016. doi:10.1364/OL.41.004803.
- [106] R. van der Meer, J. J. Renema, B. Brecht, C. Silberhorn, and P. W. H. Pinkse. “Optimizing spontaneous parametric down-conversion sources for boson sampling”. *Physical Review A*, volume 101(6):063821, 2020. doi:10.1103/PhysRevA.101.063821.
- [107] S. Paesani, M. Borghi, S. Signorini, A. Mainos, L. Pavesi, and A. Laing. “Near-ideal spontaneous photon sources in silicon quantum photonics”. *Nature Communications*, volume 11(1):2505, 2020. doi:10.1038/s41467-020-16187-8.
- [108] N. Bruno, A. Martin, T. Guerreiro, B. Sanguinetti, and R. T. Thew. “Pulsed source of spectrally uncorrelated and indistinguishable photons at telecom wavelengths”. *Optics Express*, volume 22(14):17246–17253, 2014. doi:10.1364/OE.22.017246.
- [109] T. Guerreiro, A. Martin, B. Sanguinetti, N. Bruno, H. Zbinden, and R. T. Thew. “High efficiency coupling of photon pairs in practice”. *Optics Express*, volume 21(23):27641–27651, 2013. doi:10.1364/OE.21.027641.
- [110] A. Zeilinger, M. A. Horne, H. Weinfurter, and M. Żukowski. “Three-particle entanglements from two entangled pairs”. *Physical Review Letters*, volume 78(16):3031–3034, 1997. doi:10.1103/PhysRevLett.78.3031.

- [111] C.-Y. Lu, X.-Q. Zhou, O. Gühne, W.-B. Gao, J. Zhang, Z.-S. Yuan, A. Goebel, T. Yang, and J.-W. Pan. “Experimental entanglement of six photons in graph states”. *Nature Physics*, volume 3(2):91–95, 2007. doi:10.1038/nphys507.
- [112] Z. Zhao, Y.-A. Chen, A.-N. Zhang, T. Yang, H. J. Briegel, and J.-W. Pan. “Experimental demonstration of five-photon entanglement and open-destination teleportation”. *Nature*, volume 430(6995):54–58, 2004. doi:10.1038/nature02643.
- [113] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger. “Experimental demonstration of four-photon entanglement and high-fidelity teleportation”. *Physical Review Letters*, volume 86(20):4435–4438, 2001. doi:10.1103/PhysRevLett.86.4435.
- [114] P. Walther, M. Aspelmeyer, and A. Zeilinger. “Heralded generation of multiphoton entanglement”. *Physical Review A*, volume 75(1):012313, 2007. doi:10.1103/PhysRevA.75.012313.
- [115] V. Saggio, A. Dimić, C. Greganti, L. A. Rozema, P. Walther, and B. Dakić. “Experimental few-copy multipartite entanglement detection”. *Nature Physics*, volume 15(9):935–940, 2019. doi:10.1038/s41567-019-0550-4.
- [116] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, *et al.* “18-qubit entanglement with six photons’ three degrees of freedom”. *Physical Review Letters*, volume 120(26):260502, 2018. doi:10.1103/PhysRevLett.120.260502.
- [117] M. Proietti, A. Pickston, F. Graffitti, P. Barrow, D. Kundys, C. Branciard, M. Ringbauer, and A. Fedrizzi. “Experimental test of local observer independence”. *Science Advances*, volume 5(9):eaaw9832, 2019. doi:10.1126/sciadv.aaw9832.
- [118] M. A. Broome, M. P. Almeida, A. Fedrizzi, and A. G. White. “Reducing multiphoton rates in pulsed down-conversion by temporal multiplexing”. *Optics Express*, volume 19(23):22698–22708, 2011. doi:10.1364/OE.19.022698.
- [119] M. Fiorentino, G. Messin, C. E. Kuklewicz, F. N. C. Wong, and J. H. Shapiro. “Generation of ultrabright tunable polarization entanglement without spatial, spectral, or temporal constraints”. *Physical Review A*, volume 69(4):041801, 2004. doi:10.1103/PhysRevA.69.041801.
- [120] P. G. Kwiat, P. H. Eberhard, A. M. Steinberg, and R. Y. Chiao. “Proposal for a loophole-free Bell inequality experiment”. *Physical Review A*, volume 49(5):3209–3220, 1994. doi:10.1103/PhysRevA.49.3209.
- [121] T. Kim, M. Fiorentino, and F. N. C. Wong. “Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer”. *Physical Review A*, volume 73(1):012316, 2006. doi:10.1103/PhysRevA.73.012316.
- [122] A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger. “A wavelength-tunable fiber-coupled source of narrowband entangled photons”. *Optics Express*, volume 15(23):15377–15386, 2007. doi:10.1364/OE.15.015377.

- [123] D. Smith. “High-efficiency quantum photonics”, 2014. doi:10.14264/uql.2015.235.
- [124] D. E. Browne and T. Rudolph. “Resource-efficient linear optical quantum computation”. *Physical Review Letters*, volume 95(1):010501, 2005. doi:10.1103/PhysRevLett.95.010501.
- [125] M. A. Nielsen. “Optical quantum computation using cluster states”. *Physical Review Letters*, volume 93(4):040503, 2004. doi:10.1103/PhysRevLett.93.040503.
- [126] E. Knill, R. Laflamme, and G. J. Milburn. “A scheme for efficient quantum computation with linear optics”. *Nature*, volume 409(6816):46–52, 2001. doi:10.1038/35051009.
- [127] M. Varnava, D. E. Browne, and T. Rudolph. “How good must single photon sources and detectors be for efficient linear optical quantum computation?” *Physical Review Letters*, volume 100(6):060502, 2008. doi:10.1103/PhysRevLett.100.060502.
- [128] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi. “Experimental quantum conference key agreement”. *Science Advances*, volume 7(23):eabe0395, 2021. doi:10.1126/sciadv.abe0395.
- [129] P. W. Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. *SIAM Journal on Computing*, volume 26(5):1484–1509, 1997. doi:10.1137/S0097539795293172.
- [130] R. L. Rivest, A. Shamir, and L. Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. *Communications of the ACM*, volume 21(2):120–126, 1978. doi:10.1145/359340.359342.
- [131] D. J. Bernstein and T. Lange. “Post-quantum cryptography”. *Nature*, volume 549(7671):188–194, 2017. doi:10.1038/nature23461.
- [132] S. Pirandola, S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, *et al.* “Advances in quantum cryptography”. *Advances in Optics and Photonics*, volume 12(4):1012–1236, 2020. doi:10.1364/AOP.361502.
- [133] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan. “Secure quantum key distribution with realistic devices”. *Reviews of Modern Physics*, volume 92(2):025002, 2020. doi:10.1103/RevModPhys.92.025002.
- [134] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. “Quantum cryptography”. *Reviews of Modern Physics*, volume 74(1):145–195, 2002. doi:10.1103/RevModPhys.74.145.
- [135] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. “The security of practical quantum key distribution”. *Reviews of Modern Physics*, volume 81(3):1301–1350, 2009. doi:10.1103/RevModPhys.81.1301.
- [136] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. *Nature*, volume 299(5886):802–803, 1982. doi:10.1038/299802a0.

- [137] P. W. Shor and J. Preskill. “Simple proof of security of the BB84 quantum key distribution protocol”. *Physical Review Letters*, volume 85(2):441–444, 2000. doi:10.1103/PhysRevLett.85.441.
- [138] D. Mayers. “Unconditional security in quantum cryptography”. *arXiv:quant-ph/9802025*, 2004.
- [139] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. “A proof of the security of quantum key distribution (extended abstract)”. In “Proceedings of the thirty-second annual ACM symposium on Theory of computing”, STOC ’00, pages 715–724. Association for Computing Machinery, 2000. doi:10.1145/335305.335406.
- [140] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. “Mixed-state entanglement and quantum error correction”. *Physical Review A*, volume 54(5):3824–3851, 1996. doi:10.1103/PhysRevA.54.3824.
- [141] A. R. Calderbank and P. W. Shor. “Good quantum error-correcting codes exist”. *Physical Review A*, volume 54(2):1098–1105, 1996. doi:10.1103/PhysRevA.54.1098.
- [142] C. E. Shannon. “A mathematical theory of communication”. *Bell System Technical Journal*, volume 27(3):379–423, 1948. doi:10.1002/j.1538-7305.1948.tb01338.x.
- [143] F. Grasselli, H. Kampermann, and D. Bruß. “Finite-key effects in multipartite quantum key distribution protocols”. *New Journal of Physics*, volume 20(11):113014, 2018. doi:10.1088/1367-2630/aaec34.
- [144] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß. “Multi-partite entanglement can speed up quantum key distribution in networks”. *New Journal of Physics*, volume 19(9):093012, 2017. doi:10.1088/1367-2630/aa8487.
- [145] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß. “Quantum Conference Key Agreement: A Review”. *Advanced Quantum Technologies*, volume 3(11):2000025, 2020. doi:10.1002/qute.202000025. ArXiv: 2003.10186.
- [146] A. Dahlberg, J. Helsen, and S. Wehner. “Transforming graph states to bell-pairs is NP-complete”. *Quantum*, volume 4:348, 2020. doi:10.22331/q-2020-10-22-348.
- [147] A. Dahlberg, J. Helsen, and S. Wehner. “How to transform graph states using single-qubit operations: computational complexity and algorithms”. *arXiv:1805.05306 [quant-ph]*, 2018.
- [148] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White. “Measurement of qubits”. *Physical Review A*, volume 64(5):052312, 2001. doi:10.1103/PhysRevA.64.052312.
- [149] Z. Hradil. “Quantum-state estimation”. *Physical Review A*, volume 55(3):R1561–R1564, 1997. doi:10.1103/PhysRevA.55.R1561.
- [150] O. Gühne and G. Tóth. “Entanglement detection”. *Physics Reports*, volume 474(1):1–75, 2009. doi:10.1016/j.physrep.2009.02.004.

- [151] Y. Tokunaga, T. Yamamoto, M. Koashi, and N. Imoto. “Fidelity estimation and entanglement verification for experimentally produced four-qubit cluster states”. *Physical Review A*, volume 74(2):020301, 2006. doi:10.1103/PhysRevA.74.020301.
- [152] R. D. Somma, J. Chiaverini, and D. J. Berkeland. “Lower bounds for the fidelity of entangled-state preparation”. *Physical Review A*, volume 74(5):052302, 2006. doi:10.1103/PhysRevA.74.052302.
- [153] C.-Y. Lu, W.-B. Gao, O. Gühne, X.-Q. Zhou, Z.-B. Chen, and J.-W. Pan. “Demonstrating anyonic fractional statistics with a six-qubit quantum simulator”. *Physical Review Letters*, volume 102(3):030502, 2009. doi:10.1103/PhysRevLett.102.030502.
- [154] J. C. Adcock, C. Vigliar, R. Santagati, J. W. Silverstone, and M. G. Thompson. “Programmable four-photon graph states on a silicon chip”. *Nature Communications*, volume 10(1):3528, 2019. doi:10.1038/s41467-019-11489-y.
- [155] C. Vigliar, S. Paesani, Y. Ding, J. C. Adcock, J. Wang, S. Morley-Short, D. Bacco, L. K. Oxenløwe, M. G. Thompson, *et al.* “Error protected qubits in a silicon photonic chip”. *arXiv:2009.08339 [physics, physics:quant-ph]*, 2020.
- [156] D. Donoho. “Compressed sensing”. *IEEE Transactions on Information Theory*, volume 52(4):1289–1306, 2006. doi:10.1109/TIT.2006.871582.
- [157] R. L. Kosut. “Quantum Process Tomography via L1-norm Minimization”. *arXiv:0812.4323 [quant-ph]*, 2009.
- [158] D. Gross, Y.-K. Liu, S. T. Flammia, S. Becker, and J. Eisert. “Quantum State Tomography via Compressed Sensing”. *Physical Review Letters*, volume 105(15):150401, 2010. doi:10.1103/PhysRevLett.105.150401.
- [159] C. Thalacker, F. Hahn, J. de Jong, A. Pappa, and S. Barz. “Anonymous and secret communication in quantum networks”. *arXiv:2103.08722 [quant-ph]*, 2021.
- [160] F. Hahn, J. de Jong, and A. Pappa. “Anonymous Quantum Conference Key Agreement”. *PRX Quantum*, volume 1(2):020325, 2020. doi:10.1103/PRXQuantum.1.020325. ArXiv: 2010.04534.
- [161] P. Singkanipa and P. Kok. “Quantum Conference Key Agreement with Photon Loss”. *arXiv:2101.01483 [quant-ph]*, 2021.
- [162] C. Taballione, R. van der Meer, H. J. Snijders, P. Hooijschuur, J. P. Epping, M. de Goede, B. Kassenberg, P. Venderbosch, C. Toebes, *et al.* “A universal fully reconfigurable 12-mode quantum photonic processor”. *Materials for Quantum Technology*, volume 1(3):035002, 2021. doi:10.1088/2633-4356/ac168c.
- [163] C. Branciard, D. Rosset, Y.-C. Liang, and N. Gisin. “Measurement-Device-Independent Entanglement Witnesses for All Entangled Quantum States”. *Physical Review Letters*, volume 110(6), 2013. doi:10.1103/PhysRevLett.110.060405.

- [164] Z.-D. Li, Q. Zhao, R. Zhang, L.-Z. Liu, X.-F. Yin, X. Zhang, Y.-Y. Fei, K. Chen, N.-L. Liu, *et al.* “Measurement-Device-Independent Entanglement Witness of Tripartite Entangled States and Its Applications”. *Physical Review Letters*, volume 124(16):160503, 2020. doi:10.1103/PhysRevLett.124.160503.
- [165] M. Ho, P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard. “Noisy pre-processing facilitating a photonic realisation of device-independent quantum key distribution”. *Physical Review Letters*, volume 124(23), 2020. doi:10.1103/PhysRevLett.124.230502.
- [166] E. Woodhead, A. Acín, and S. Pironio. “Device-independent quantum key distribution with asymmetric CHSH inequalities”. *Quantum*, volume 5, 2021. doi:10.22331/q-2021-04-26-443.
- [167] S. Yokoyama, R. Ukai, S. C. Armstrong, C. Sornphiphatphong, T. Kaji, S. Suzuki, J.-i. Yoshikawa, H. Yonezawa, N. C. Menicucci, and A. Furusawa. “Ultra-large-scale continuous-variable cluster states multiplexed in the time domain”. *Nature Photonics*, volume 7(12):982–986, 2013. doi:10.1038/nphoton.2013.287.
- [168] W. Asavanant, Y. Shiozawa, S. Yokoyama, B. Charoensombutamon, H. Emura, R. N. Alexander, S. Takeda, J.-i. Yoshikawa, N. C. Menicucci, *et al.* “Generation of time-domain-multiplexed two-dimensional cluster state”. *Science*, volume 366(6463):373–376, 2019. doi:10.1126/science.aay2645.
- [169] M. Yukawa, R. Ukai, P. van Loock, and A. Furusawa. “Experimental generation of four-mode continuous-variable cluster states”. *Physical Review A*, volume 78(1):012301, 2008. doi:10.1103/PhysRevA.78.012301.
- [170] J.-i. Yoshikawa, S. Yokoyama, T. Kaji, C. Sornphiphatphong, Y. Shiozawa, K. Makino, and A. Furusawa. “Invited Article: Generation of one-million-mode continuous-variable cluster state by unlimited time-domain multiplexing”. *APL Photonics*, volume 1(6):060801, 2016. doi:10.1063/1.4962732.
- [171] N. C. Menicucci. “Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States”. *Physical Review Letters*, volume 112(12):120504, 2014. doi:10.1103/PhysRevLett.112.120504. Publisher: American Physical Society.
- [172] C. Maurer, C. Becher, C. Russo, J. Eschner, and R. Blatt. “A single-photon source based on a single ca^+ ion”. *New Journal of Physics*, volume 6:94–94. doi:10.1088/1367-2630/6/1/094.
- [173] P. Senellart, G. Solomon, and A. White. “High-performance semiconductor quantum-dot single-photon sources”. *Nature Nanotechnology*, volume 12(11):1026–1039, 2017. doi:10.1038/nnano.2017.218.
- [174] J. McKeever, A. Boca, A. D. Boozer, R. Miller, J. R. Buck, A. Kuzmich, and H. J. Kimble. “Deterministic generation of single photons from one atom trapped in a cavity”. *Science*, volume 303(5666):1992–1994, 2004. doi:10.1126/science.1095232.

- [175] C. Toninelli, I. Gerhardt, A. S. Clark, A. Reserbat-Plantey, S. Götzinger, Z. Ristanović, M. Colautti, P. Lombardi, K. D. Major, *et al.* “Single organic molecules for photonic quantum technologies”. *Nature Materials*, pages 1–14, 2021. doi:10.1038/s41563-021-00987-4.
- [176] S. Pazzagli, S. Pazzagli, P. Lombardi, P. Lombardi, D. Martella, M. Colautti, B. Tiribilli, F. S. Cataliotti, F. S. Cataliotti, *et al.* “Photostable single-photon emission from organic nanocrystals”. In “Conference on Lasers and Electro-Optics (2018)”, Optical Society of America, 2018. doi:10.1364/CLEO_AT.2018.JTh2A.46.
- [177] B. Lounis and W. E. Moerner. “Single photons on demand from a single molecule at room temperature”. *Nature*, volume 407(6803):491–493, 2000. doi:10.1038/35035032.
- [178] G. J. Mendoza, R. Santagati, J. Munns, E. Hemsley, M. Piekarek, E. Martín-López, G. D. Marshall, D. Bonneau, M. G. Thompson, and J. L. O’Brien. “Active temporal and spatial multiplexing of photons”. *Optica*, volume 3(2):127–132, 2016. doi:10.1364/OPTICA.3.000127.
- [179] X.-s. Ma, S. Zotter, J. Kofler, T. Jennewein, and A. Zeilinger. “Experimental generation of single photons via active multiplexing”. *Physical Review A*, volume 83(4), 2011. doi:10.1103/PhysRevA.83.043814.
- [180] T. Kiyohara, R. Okamoto, and S. Takeuchi. “Realization of multiplexing of heralded single photon sources using photon number resolving detectors”. *Optics Express*, volume 24(24), 2016. doi:10.1364/OE.24.027288.
- [181] M. J. Collins, C. Xiong, I. H. Rey, T. D. Vo, J. He, S. Shahnian, C. Reardon, T. F. Krauss, M. J. Steel, *et al.* “Integrated spatial multiplexing of heralded single-photon sources”. *Nature Communications*, volume 4(1):2582, 2013. doi:10.1038/ncomms3582.
- [182] F. Kaneda and P. G. Kwiat. “High-efficiency single-photon generation via large-scale active time multiplexing”. *Science Advances*, volume 5(10):eaaw8586, 2021. doi:10.1126/sciadv.aaw8586.
- [183] A. L. Migdall, D. Branning, and S. Castelletto. “Tailoring single-photon and multiphoton probabilities of a single-photon on-demand source”. *Physical Review A*, volume 66(5), 2002. doi:10.1103/PhysRevA.66.053805.
- [184] T. B. Pittman, B. C. Jacobs, and J. D. Franson. “Single photons on pseudodemand from stored parametric down-conversion”. *Physical Review A*, volume 66(4), 2002. doi:10.1103/PhysRevA.66.042303.
- [185] F. Buscemi. “All Entangled Quantum States Are Nonlocal”. *Physical Review Letters*, volume 108(20), 2012. doi:10.1103/PhysRevLett.108.200401.
- [186] D. Rosset, F. Buscemi, and Y.-C. Liang. “Resource Theory of Quantum Memories and Their Faithful Verification with Minimal Assumptions”. *Physical Review X*, volume 8(2), 2018. doi:10.1103/PhysRevX.8.021033.