Integrated Photonic Multiplexing for Quantum Information

BENJAMIN HAYLOCK
BPhotNan (Hons)
Centre for Quantum Dynamics
School of Environment and Science
Griffith University

Submitted in fulfilment of the requirements of the degree of Doctor of Philosophy
July 2018
Abstract

Herewithin we present multiplexed integrated photonics as a realisable route to large-scale quantum technologies. Quantum photonics is one many platforms for experimental demonstrations of quantum information science. The technological advantages afforded by the combination of integrated photonic circuits with multiplexing techniques can enable performance enhancements to make photonics a leading infrastructure for implementation of real-world quantum information systems.

For this purpose, we create integrated circuits to solve technical challenges in the fields of quantum cryptography, discrete variable and continuous variable quantum computation. These circuits were fabricated in a facility developed at Griffith University, Centre for Quantum Dynamics, for the production of annealed and reverse proton exchange waveguides in congruent lithium niobate and have found applications across the fields of quantum optics and cryptography.

We develop and demonstrate the first integrated many-mode active optical demultiplexing of single photons from a solid-state source. This scheme enables the production of a multiphoton Fock state across multiple spatial modes from a single high brightness solid-state source with temporal indistinguishability. This work addressed a major hurdle in the development of photonic quantum computers, namely generation of a large number of indistinguishable single photons on demand. To perform the demultiplexing of single photons we develop two key technologies; a high-speed 1:4 integrated photonic switch and a many channel arbitrary pulse sequence generator.

Cryptography as a field is increasingly reliant on quantum random number generators for added security. With increased demand comes a requirement for higher bitrate random number generators, and as such we demonstrate multiplexing of a random number generation scheme based on measurements of quantum vacuum fluctuations. Furthermore, we show an increased level of security at high bitrates by implementing a new signal processing scheme.

We demonstrate integrated generation, manipulation and homodyning of squeezed light on a single chip for the first time. This scheme is the first successful demonstration of full integration of all the major components needed for continuous variable quantum computation in a temporally multiplexed architecture. These results represent contributions to several fields of study, demonstrating the advantages of integrated quantum photonic multiplexing, and are of interest to the quantum computing, information security, integrated optics, and electronic control communities.
Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

(Signed)

Benjamin Haylock
## Contents

Abstract ........................................................................................................................................... ii
Statement of Originality .................................................................................................................... iii
List of Figures .................................................................................................................................. v
List of Tables ...................................................................................................................................... v
Acknowledgements ........................................................................................................................... vi
Acknowledgement of Papers included in this Thesis ........................................................................ vii
Statement on Referencing ................................................................................................................ x

1. Introduction...................................................................................................................................... 1
   1.1. Encoding quantum information in light .................................................................................. 3
       1.1.1. Photonic qubits .............................................................................................................. 4
       1.1.2. Photonic qumodes ........................................................................................................ 7
   1.2. Integrated quantum photonics .................................................................................................. 10
   1.3. Nonlinear high-speed reconfigurable integrated photonics in lithium niobate ......................... 19
   1.4. Active integrated quantum photonics .................................................................................... 23
   1.5. Photonic multiplexing for quantum information ..................................................................... 25
   1.6. Thesis structure .................................................................................................................... 28

2. Demultiplexing Single Photons ...................................................................................................... 30
   2.1. Statement of contribution to co-authored published paper .................................................. 30
   2.2. Fully integrated active optical demultiplexer ........................................................................ 31
       2.2.1. Included Paper - Active demultiplexing of single photons from a solid-state source ........ 32

3. Fast Switching Electronics ............................................................................................................. 38
   3.1. Statement of contribution to co-authored published paper .................................................. 38
   3.2. High speed arbitrary pulsed control sequences .................................................................... 39
       3.2.1. Included Paper - Nine channel mid-power bipolar pulse generator based on a field programmable gate array .................................................................................. 39

4. Multiplexed QRNG ....................................................................................................................... 43
   4.1. Statement of contribution to co-authored published Paper .................................................. 43
   4.2. Multiplexed quantum random number generation ............................................................... 44
       4.2.1. Included Paper – Multiplexed quantum random number generation .............................. 44

5. Integrated generation, manipulation and detection of squeezed light ........................................... 53
5.1. Statement of contribution to co-authored published paper........................53
5.2. Integrated generation, manipulation and homodyne detection of continuous variable entanglement.................................................................54
  5.2.1. Included Paper – Integrated photonic platform for quantum information with continuous variables...........................................................54
6. Conclusion..................................................................................................63
Appendices.....................................................................................................67
  Appendix A – List of Co-Authored Papers published during PhD not included elsewhere..............................................................................67
Bibliography...................................................................................................68

List of Figures
Figure 1 Entanglement structure needed for universal computation with the one-way quantum computing scheme......................................................6
Figure 2 Probabilistic C-NOT gate with success probability 1/9.........................11
Figure 3 Structures of various waveguide geometries......................................10
Figure 4 Schematic of a micro-pillar quantum dot............................................14
Figure 5 Periodically poled waveguide used for frequency conversion between UV and telecom wavelengths..............................................................16
Figure 6 Overview of our process flow for fabrication of non-linear, electro-optic, integrated photonic devices in lithium niobate.................................21
Figure 7 Left shows periodic poling structure for quasi-phase matching. Right shows a 40x microscope image of a part of a fabricated electrode. .......................21
Figure 8 Photographs of finished integrated photonic device in lithium niobate illuminated with red light. .................................................................22
Figure 9 Simulated electric field for an electro-optic modulator. ......................25

List of Tables
Table 1 Information Encoding Techniques......................................................4
Table 2 Progress in optical discrete variable and continuous variable quantum computation..................................................................................9
Table 3 A summary of critical information for each waveguide material platform as applicable to quantum information..............................................18
Acknowledgements

This work has been supported by the Australian Government Research Training Program Scholarship.

Firstly, I would like to acknowledge the support of my supervisor A/Prof Mirko Lobino, without whom none of this work would have been possible. Few people are lucky enough to see their supervisor daily to discuss their work, but I am one of the fortunate, and for that, I am incredibly grateful.

To all the members of the IQT photonics group: Francesco Lenzini, Sachin Kasture, Matteo Villa, Paul Fisher, Valdis Blums, Daniel Peace, and Stefan Morley thanks for your support, work and discussion before, during and after being members of the group. I want to thank all collaborating authors for their hard work and thoughtful discussion.

I would also like to thank all my friends, family, teachers, and lecturers for their guidance and support. In particular, I would like to thank my parents Bob and Sharon, and my sister Marita for always being there for me, encouraging, reminding, helping, and loving me.
Acknowledgement of Papers included in this Thesis

Section 9.1 of the Griffith University Code for the Responsible Conduct of Research (“Criteria for Authorship”), in accordance with Section 5 of the Australian Code for the Responsible Conduct of Research, states:

To be named as an author, a researcher must have made a substantial scholarly contribution to the creative or scholarly work that constitutes the research output, and be able to take public responsibility for at least that part of the work they contributed. Attribution of authorship depends to some extent on the discipline and publisher policies, but in all cases, authorship must be based on substantial contributions in a combination of one or more of:

- conception and design of the research project
- analysis and interpretation of research data
- drafting or making significant parts of the creative or scholarly work or critically revising it so as to contribute significantly to the final output.

Section 9.3 of the Griffith University Code (“Responsibilities of Researchers”), in accordance with Section 5 of the Australian Code, states:

Researchers are expected to:

Offer authorship to all people, including research trainees, who meet the criteria for authorship listed above, but only those people.

- Accept or decline offers of authorship promptly in writing.
- Include in the list of authors only those who have accepted authorship
- Appoint one author to be the executive author to record authorship and manage correspondence about the work with the publisher and other interested parties.
- Acknowledge all those who have contributed to the research, facilities or materials but who do not qualify as authors, such as research assistants, technical staff, and advisors on cultural or community knowledge. Obtain written consent to name individuals.

Included in this thesis are papers in Chapters 2, 3, 4 and 5, which are co-authored with other researchers. My contribution to each co-authored paper is outlined at the front of the relevant chapter. The bibliographic details and publication status for these papers including all authors are:
Chapter 2, Section 2.1:

This paper is reproduced here under a copyright license agreement between Mr. Benjamin Haylock and John Wiley and Sons under the terms and conditions provided by John Wiley and Sons and Copyright Clearance Center, license number 4357550480300.

(Signed)  
(Date) 27/07/2018  
Benjamin Haylock  

(Countersigned)  
(Date) 27/07/2018  
Supervisor: Mirko Lobino

Chapter 3, Section 2.1:

This paper is reproduced here under a copyright license agreement between Mr. Benjamin Haylock and AIP Publishing under the terms and conditions provided by AIP Publishing and Copyright Clearance Center, license number 4357551336081.

(Signed)  
(Date) 27/07/2018  
Benjamin Haylock  

(Countersigned)  
(Date) 27/07/2018  
Supervisor: Mirko Lobino
Chapter 4, Section 2.1:


(Signed) (Date) 27/07/2018
Benjamin Haylock
(Countersigned) (Date) 27/07/2018
Supervisor: Mirko Lobino

Chapter 5, Section 2.1:

Francesco Lenzini, Jiri Janousek, Oliver Thearle, Ben Haylock, Matteo Villa, Sachin Kasture, Liang Cui, Hoang-Phuong Phan, Dzung Viet Dao, Hidehiro Yonezawa, Ping Koy Lam, Elanor Huntington, and Mirko Lobino, “Integrated photonic platform for quantum information with continuous variables” submitted to Science Advances

(Signed) (Date) 27/07/2018
Benjamin Haylock
(Countersigned) (Date) 27/07/2018
Supervisor: Mirko Lobino

Appropriate acknowledgements of those who contributed to the research but did not qualify as authors are included in each paper.
Statement on Referencing

Within this document, where a publication is included, the references, and referencing system used in that paper is wholly retained unaltered. Throughout the remainder of the document, for those sections that are not direct insertions of a publication, the references are compiled at the end of the document into a single bibliography.
1. Introduction

As every scientific endeavour matures, focus inevitably shifts from inquiry to application. Quantum physics is no exception, and the landmark discoveries of the 19th and 20th centuries\(^1\) led to theoretical debate, and experimental demonstration of many of its founding principles. From fundamental principles of quantum mechanics such as the no-cloning theorem\(^2\) and non-locality\(^3\), came the idea of secure communication. Theoretical discoveries in the 1990's of quantum computing algorithms with better scalability than known classical algorithms led to a surge in interest in using quantum physics to solve real-world problems. These include Shor’s algorithm for factoring prime numbers\(^4\), Grover’s database search algorithm\(^5,6\), and quantum simulation\(^7,8\).

Over the past two decades, experimental research has led to many exciting new quantum technologies in diverse fields such as communication\(^9\), computation\(^10\), cryptography\(^11\), sensing\(^12\) and simulation\(^13\). Naturally, initial demonstrations of possible practical uses has led to significant investment in the field, and, with it, a drive to improve the performance of such systems. For quantum computation, this means increasing computational power to extend the complexity of the operation the system can perform. For quantum communication and cryptography, it means creating faster and more secure methods of data transfer across increasingly large distances\(^14-16\).

There are numerous platforms used for quantum applications, including systems comprising single atoms\(^17,18\), ions\(^19\), spins\(^20-22\), superconducting circuits\(^23\), optical\(^24,25\) and microwave photons\(^26\), as well as multi-particle systems such as molecules\(^27-29\), collective spin excitations of atomic clouds\(^30\), and the modes of optical\(^31,32\) and microwave\(^33\) quantum harmonic oscillators. While the proliferation of physical bases is evidence that no single system has yet resolved all of its issues, quantum optics is one of the most developed fields of quantum information. The advanced level of experimental knowledge makes quantum optics our choice for new investigations.

Photonics is a natural choice for quantum communication systems, as it allows for high speed, high fidelity transmission of information across vast distances. The encoding and preservation of quantum information in light presents its own
challenges, however much progress has been made towards this with demonstrations of satellite to ground quantum key distribution\textsuperscript{11} and metropolitan network quantum teleportation\textsuperscript{34}. Nonetheless quantum communication still faces practical challenges for its extensibility\textsuperscript{35}.

The search for the best system for quantum computing is unresolved with many systems investigated for this purpose\textsuperscript{36}. At the heart of the technological problem lies the difficulty that quantum information carriers must interact readily with other quantum information carriers in a controlled manner for the desired operations to occur, without interacting with the environment, to reduce decoherence and loss of information. A universal quantum computer can be constructed using numerous different combinations of quantum logic gates, but common to all constructions is the need for at least one single qubit and one multiple qubit logic operation. This multiple input gate is the operation that requires an interaction between quantum information carriers.

Those that wish to use light to encode their quantum information take two separate approaches based on this problem, namely photonic qubits, and photonic qumodes. The two approaches offer high environmental immunity, and simple interactions with other quantum information carriers respectively, but struggle with the second criterion. These methods and solutions to make them viable standards for quantum computing are discussed in more detail in Section 1.1.

Our approach towards finding technological solutions comes from the standpoint of integration. Integration drives increases in performance by enabling reliable repeated production of a component or device, allowing construction of more complex systems from subsystems previously considered the limit of technological capabilities. Indeed many of the players at the forefront of the quantum technology race, such as IBM\textsuperscript{37}, Microsoft\textsuperscript{38}, Rigetti\textsuperscript{39,40}, and IDQuantique\textsuperscript{41}, are drawing on their integration expertise to make progress in their efforts. Photonic platforms have played a considerable role in the demonstration of quantum phenomena, and a considerable body of work has investigated integrating optical components and circuits in a similar way to electronic devices and microchips. Indeed, within the last couple of years a number of optical quantum computing start-ups have formed\textsuperscript{42,43}, and commercial quantum communications systems using light\textsuperscript{44,45} continue to thrive.
The focus of our work is to use photonic multiplexing techniques to extend the capabilities of quantum information systems. We address key experimental problems in this way. The first such problem is the bitrate of quantum communications. We experimentally demonstrate a spatially multiplexed quantum random number generation scheme suitable for providing the volumes of randomness required for the encryption step of next generation systems, thus enabling increases in their bitrates. Our second focus is on increasing the rates of single photon sources for discrete variable quantum computation protocols through high speed photonic temporal multiplexing. Finally, we focus on integration of all the key components necessary to demonstrate the fundamental elements for continuous variable quantum computation. This circuit requires temporal multiplexing of quantum light sources. With extensibility of this scheme already demonstrated, we work towards providing a technological solution to create a large, universal quantum computer.

In the remainder of this chapter, a review of quantum information encoding in light is presented before an overview of previous work on integration of quantum photonics is made as background for the results presented here. A discussion on actively reconfigurable integrated photonic circuits is undertaken, and a description of the fabrication process used to achieve these goals is completed. Finally, previous experimental implementations of optical multiplexing for quantum optics are presented as background for this work.

1.1. Encoding quantum information in light

Classically we can think of encoding information in a number of ways. Our counting system and classical computers have made decimal and binary representations popular. These are equivalent to encoding onto a subset of the real integers, \( \mathbb{Z} \). We could choose any subset of \( \mathbb{Z} \) to encode our information on. However, we may also choose to expand our selection to encode on the real number line, \( \mathbb{R} \). These two scenarios are called digital and analogue information respectively.

Quantum information is encoded into qubits, qudits and qumodes in analogy with binary digital, arbitrary size digital and analogue classical information respectively. The possible measurement outcomes from each of these quantum information encodings are exactly the analogous classical information.
Theoretically discrete and continuous encoding techniques, are not equivalent, i.e. information in R cannot be encoded using Z. However, in a real system, measurements have a finite resolution, meaning analogue information is always digitised into a finite number of outcomes. Nonetheless, we can treat this approximation to continuity in a continuous framework. The utilisation of qubits and qumodes for quantum communication and computation differs significantly, with each scheme having distinct advantages and disadvantages. Single particle systems and systems with quantised energy levels such as atoms, photons and ions naturally fit into discrete variable frameworks, whereas collective excitations and modes of fields are in the continuous variable regime. The ways of experimentally implementing discrete variable (qubit) and continuous variable (qumode) protocols using photonics differ significantly, as described below.

Table 1 Information Encoding Techniques

<table>
<thead>
<tr>
<th>Measurement Outcome</th>
<th>Classical Information</th>
<th>Quantum Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I \subset \mathbb{Z} = [0,1]$</td>
<td>Digital - Binary</td>
<td>Qubits</td>
</tr>
<tr>
<td>$I \subset \mathbb{Z} = [0,d]$</td>
<td>Digital – Decimal, Hex etc.</td>
<td>Qudits</td>
</tr>
<tr>
<td>$I \subset \mathbb{R}$ $= (-\infty, \infty)$</td>
<td>Analogue</td>
<td>Qumodes</td>
</tr>
</tbody>
</table>

1.1.1. Photonic qubits

The discrete variable approach uses single photons, encoding information in any of its discrete degrees of freedom such as polarisation, orbital angular momentum, path, time-bin, frequency-bin, temporal mode, or photon number. The states of interest are usually represented in the number basis, i.e. one polarisation, path, frequency etc. is denoted with the $|0\rangle$ state and the others as others as $|n\rangle$ states. Single qubit operations are performed by optical elements transforming the state of the single photon.

\footnote{Note that these are not Fock states, with the exception of photon number encoding, and $|0\rangle$ is not the vacuum state. Indeed the case of a lost photon is normally ignored.}

---

4
photon. Two qubit operations require the interaction of two single photons; however, this is extremely difficult due to the lack of a strong photon-photon interaction. Instead, other schemes allow two qubit operations to be performed probabilistically or through strong coupling to interacting systems. Measurements are completed by projecting the state into a path encoding and measuring a single photon in a specific spatial mode. The complete state description is usually represented with a density matrix in the number basis.

Most of these approaches ensure there is no loss of information to the environment, as single photons are highly immune to decoherence, and either the photon is lost, or the state is preserved with very high fidelity. Unfortunately it is extremely difficult to make the quantum information encoded on single photons interact with other photons as required for a fully photonic quantum computing architecture. Indeed such interactions have only recently been experimentally achieved with single atoms in optical cavities46. Fortunately, theoretical and experimental work has shown that scalable universal quantum computation is possible with only linear optical networks, single photon sources, single photon detectors, and feedforward operations47,48. This protocol is known as linear optical quantum computation (LOQC). For an in depth review of linear optical quantum computing see Kok et al.24.

These discoveries have shown a path forward for discrete variable photonic quantum computing. However, resource overhead challenges require resolution before successful large-scale implementations are possible.

One way quantum computing has been proposed as an alternative approach to the quantum logic gate based model of universal quantum computation with qubits49. Often called cluster-state or measurement-based quantum computation this process uses large arrays of photons with complex entanglement structures (see Figure 1) as the fundamental resource and requires only single qubit operations, measurement, and feedforward to perform universal quantum computation. Experimental implementations50–53 have been limited by their ability to generate the necessary 2D cluster state of sufficient size. Though larger 1D cluster states have been generated with deterministic entangling operations, these are not suitable for universal quantum computation54. A theoretical proposal exists for extending this deterministic entangling operation, based on a precessing spin in a quantum dot, to two
The lack of a deterministic two-qubit gate using only linear optics causes experimental difficulties for this scheme, however non-deterministic cluster state preparation is sufficient for scalability. This assumption of scalability relies on sufficient source and detector efficiencies. In the ideal scenario, where the photonic circuit is lossless the product of single photon source brightness and detector efficiency must be greater than \( \frac{2}{3} \) for a scalable construction of a linear optical quantum computer.

Brightness is defined as the probability of obtaining a single photon on demand, and detector efficiency the probability that a photon incident on a detector is measured. Single photon detectors with efficiencies up to 85% are now commercially available, and in the laboratory higher efficiencies have been observed, up to 99%. This means for a scalable linear optical quantum computer, three main challenges remain, namely, single photon sources with efficiencies greater than \( \frac{0.67}{85}\% = 78\% \), large, low loss linear optical networks, and fast feedforward operations. In a realistic scenario, where the photonic circuit is lossy, the single photon indistinguishability is not unity, and multi-photon probability is finite, this limit will be higher. These are all challenges that integrated photonics aims to address.

Boson sampling, a non-universal quantum computation has been described as a method that does not require two qubit gates. It is another promising proposal towards showing a genuine quantum advantage, i.e. a computational task that a quantum computer performs faster than any classical supercomputer; although recent work has increased the size of the quantum system necessary to reach this limit.

Figure 1 Entanglement structure needed for universal computation with the one-way quantum computing scheme. It is known as a 2D cluster state or 2D graph state, with each yellow node representing a qubit, and each black line denoting qubits with which it is entangled.
1.1.2. Photonic qumodes

The second approach encodes information in the optical field, using continuous variables, namely the canonical position ($\hat{q}$) and momentum ($\hat{p}$) operators of the quantum harmonic oscillator that describes the electromagnetic field. The standard basis states used are the unbounded non-physical quadrature states $|q\rangle$ and $|p\rangle$, eigenstates of their respective operators. Measurements are performed by homodyne detection\(^6\). The state is commonly described using a Wigner function\(^6\), q-function, p-function, or other s-parameterised quasiprobability distributions\(^6\). Single qumode operations are performed by phase rotations and either squeezing or shearing operations, most commonly squeezing.

Squeezing is described by the squeezing parameter\(^6\), $\zeta$, which alters the variance of the distributions in $|q\rangle$ and $|p\rangle$ according to\(^b\):

$$\Delta^2 q = \frac{1}{2} e^{-2\zeta}, \Delta^2 p = \frac{1}{2} e^{2\zeta}$$

In other words squeezing reduces the noise variance in one quadrature below that of vacuum\(^5\), and increases the noise variance in the other quadrature, maintaining a minimum uncertainty state by keeping the product $\Delta q \Delta p$ constant. Squeezed vacuum is experimentally deterministically generated by spontaneous parametric down conversion\(^6\).

Two qumode operations are markedly simpler than two qubit operations, and implemented with a beamsplitter. This approach ensures desired interactions occur deterministically. However, in this scenario optical loss becomes equivalent to a two qumode operation with vacuum as one input, acting as a decoherence source to the state of interest.

Continuous variables have been shown to be suitable for quantum computation purposes\(^6\). However known error correction techniques are not suitable for qumodes, instead requiring the embedded encoding of a qubit into the mode. This can be achieved in a number of ways, most famously using the Gottesman-Kitaev-\

\(^b\) Setting $\hbar=1$

\(^*\) $\Delta^2 q = \Delta^2 p = 0.5$ for the vacuum state
Preskill encoding\textsuperscript{68}. Using cluster state\textsuperscript{49} techniques with this encoding enabled proof of an error-correctable universal quantum computer using continuous variables\textsuperscript{69}. A fault tolerance threshold has been determined based on the size of the squeezing parameter required\textsuperscript{70}, and later revised to allow more loss\textsuperscript{71}.

Unlike discrete variables, two-qumode gates are deterministic, allowing for deterministic generation of continuous variable analogues of cluster states\textsuperscript{72}. In this case, the nodes of the structure contain qumodes rather than qubits. For universal quantum computation, some nodes of the structure and some measurements must be non-Gaussian states, which increases experimental difficulty.

An implementation of a universal quantum computer with continuous variables, capable of arbitrarily large computations has been proposed using only four quantum state sources, two delay lines, four beamsplitters, and four detectors\textsuperscript{73}. Therefore, continuous variable quantum computing does not suffer from the tyranny of numbers. Instead, the performance of each of these elements pose the challenge that integrated optics must attempt to solve. Phase rotations require maintenance of phase stability relative to a reference beam. Phase stability is a problem intrinsically solved by the monolithic nature of integrated optics. Losses in the optical system also limit the size of the cluster over which fault tolerant quantum computing can be performed, and is a problem that integrated optics offers little advantage in comparison to bulk optics, with improved mode overlap more than cancelled out by increased propagation losses. The long interaction lengths and strong mode confinement of waveguides enhances available nonlinearity for potentially generating higher squeezing levels. Due to waveguide losses however, the largest demonstrated amounts of squeezing have been created off-chip\textsuperscript{74}.

A comparison of the advances made in the two approaches is presented in Table 2. It is not designed to be complete, and lacks the detailed discussion undertaken in the text and the many individual papers on each topic, but presents an overview of both progress and challenges for universal photonic quantum computing to reach large-scale implementations.
<table>
<thead>
<tr>
<th>Discrete Variable</th>
<th>Continuous Variable</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fault tolerant large scale universal quantum computing requirements</strong></td>
<td></td>
</tr>
<tr>
<td>• Error-correctable encoding available</td>
<td></td>
</tr>
<tr>
<td>• Scalability demonstrated</td>
<td></td>
</tr>
<tr>
<td>• Sources needed</td>
<td></td>
</tr>
<tr>
<td>• Photonic circuits needed</td>
<td></td>
</tr>
<tr>
<td>• Detectors available – further integration needed</td>
<td></td>
</tr>
<tr>
<td>• Measurement and feedforward needed</td>
<td></td>
</tr>
<tr>
<td><strong>Attributes</strong></td>
<td></td>
</tr>
<tr>
<td>High fidelity operations</td>
<td>Loss dependent fidelity</td>
</tr>
<tr>
<td>Probabilistic operation</td>
<td>Deterministic operation</td>
</tr>
<tr>
<td>Experimentally simple encoding</td>
<td>Experimentally complex encoding</td>
</tr>
<tr>
<td>Resource heavy two-qubit gates</td>
<td>Simple two-qumode gates</td>
</tr>
<tr>
<td>Experimentally implemented single and two-qubit gates (^{48}), including integration (^{75})</td>
<td>No experimentally implemented gates with fault tolerant encoding.</td>
</tr>
<tr>
<td>16x16 dimensional entanglement demonstrated (^{76})</td>
<td>Million mode entanglement demonstrated (^{78})</td>
</tr>
<tr>
<td>(2^{18}) dimensional entanglement demonstrated (^{77})</td>
<td></td>
</tr>
</tbody>
</table>
1.2. Integrated quantum photonics

Integration has enabled considerable extension to the complexity of demonstrations of quantum photonics. Issues that can be solved by integration plague bulk optics experiments and depending on the application these include, phase stability, mode overlap, modulation speed and nonlinear efficiency, as well as practical concerns such as component size, cost, and wear rate, alignment stability, setup time, and ruggedness. Presently no single material is problem free; hence, there is a proliferation of research across many materials as well as research into new, promising substrates, and hybrid combinations of materials. As numerous in depth reviews exist on this topic, what follows is only a brief discussion of several of the major material platforms used in quantum applications.

Silica and glass based approaches were among the earliest demonstrations of integrated quantum photonics, with their ease of fabrication proving appealing. However, their lack of a large electro-optic coefficient, or a strong optical nonlinearity has led to them largely being used as passive photonic interconnects, with their large size preventing fabrication of circuits with large network depths. Waveguides in silica are usually made as either rib or ridge structures using a silica on silicon wafer, whereas waveguides in glass are usually made by laser writing or doping as shown in Figure 2. The first integration of quantum key distribution functionalities was done with a silica Mach-Zehnder interferometer in 2004. The stability of an integrated circuit enabled reliable measurement of phase-encoded quantum information.

![Figure 2 Structures of various waveguide geometries, from left to right, planar lightwave circuit (PLC), rib waveguide, ridge/nanowire, doped or laser written waveguide. Black dotted line shows approximate guided fundamental mode.](image)

Figure 2 Structures of various waveguide geometries, from left to right, planar lightwave circuit (PLC), rib waveguide, ridge/nanowire, doped or laser written waveguide. Black dotted line shows approximate guided fundamental mode.
In 2008, Politi et al. showed quantum interference and high fidelity C-NOT gate operation in silica ridge waveguides\textsuperscript{75}. The C-NOT gate was made with a linear optical post-selected architecture shown in Figure 3 as proposed by Ralph et al. and has a success probability of $1/9^{87}$. In follow-up work they use this circuit to perform a small compiled version of Shor’s algorithm\textsuperscript{88}, and others have shown C-NOT gates for polarisation qubits in glass\textsuperscript{89}. These experiments all relied on the potential for increased photonic circuit complexity through integration to simplify the implementation from the previous bulk-optical demonstration\textsuperscript{48}. Carolan et al. demonstrated a reconfigurable six mode arbitrary unitary network made with a Germania doped silica waveguide fabricated with the planar lightwave circuit (PLC) method as shown in Figure 2. The authors utilised it for simple computational and simulation tasks\textsuperscript{13,90}. This network is created with a series of thermo-optic phase shifters in a set of 15 cascaded Mach-Zehnder interferometers arranged according to the design of Reck et al.\textsuperscript{91}.

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{fig3}
\caption{Probabilistic C-NOT gate with success probability $1/9^{87}$. Yellow cubes represent beamsplitters with reflectivity 1/2; green cubes represent beamsplitters with reflectivity 1/3. Ancilla modes labelled $A_C$ and $A_T$. Qubits are path encoded, with $C_0$ representing the mode occupied when the control qubit is in the $|0\rangle$ state, and so on for other control mode $C_1$ and two target modes $T_0$ and $T_1$.}
\end{figure}

There have also been several quantum walk experiments with silica and glass, and these have been used for simulations of other quantum systems\textsuperscript{92-95}. Photonic quantum walks rely on the complexity of integrated circuits, as they require many coupled spatial modes, which can be achieved with an array of evanescently coupled waveguides, but in free space would require the alignment of many separate components and laser beams. Similarly to quantum walks, boson sampling relies on
the interaction of many spatial or temporal modes and thus integrated photonics provides enhanced technological capability. A three photon, six-mode boson sampling experiment has been performed, with silica-on-silicon waveguides used to implement the linear optical unitary.\textsuperscript{96}

Demonstrations of continuous variable entanglement\textsuperscript{97} and quantum teleportation\textsuperscript{98} have also been done in silica, making it the platform with the largest base of important results. Continuous variable quantum information is experimentally reliant on phase stability, making integration the only option for all but the simplest systems. Recently, single and entangled photon generation in silica has been shown in a range of contexts\textsuperscript{99–102}. Furthermore Calkins et al. have demonstrated high efficiency photon number resolving detectors integrated with laser written silica-on-silicon waveguides\textsuperscript{103}. The detectors are made using transition edge sensors, limiting their maximum speed to the MHz range.

Silicon nitride and silicon oxynitride offer similar advantages to silica, with low absorption loss at telecom wavelengths and transmission of visible light, but it also lacks demonstrated CMOS compatibility. They were used for the first demonstrations of quantum walks across up to 21 coupled waveguides\textsuperscript{104}. Together with gallium arsenide single photon sources they have been used to demonstrate integrated indistinguishable independent single emitters\textsuperscript{105}. Their high third order nonlinearity allows for efficient frequency conversion experiments\textsuperscript{106}. Recently, stoichiometric silicon nitride waveguides have been used to implement an 8x8 thermally reconfigurable network of beamsplitters and phase shifters with 128 tunable elements. It was used to show on chip quantum interference, and a single qudit gate in a spatially encoded system with dimension eight\textsuperscript{107}, but its utility is limited by lack of on chip sources and high in-coupling loss.

Work on silica and silicon nitride has largely been superseded by silicon photonics.\textsuperscript{79} Silicon has much smaller devices due to its higher refractive index contrast, and also a stronger third order nonlinearity, enabling compact single photon sources.\textsuperscript{79} Silicon, silicon nitride, and silicon oxynitride waveguides are usually fabricated as either nanowire or rib waveguides (see Figure 2) on a silicon on insulator (SOI) wafer.

Silicon is the most developed platform for quantum applications,\textsuperscript{108} and the closest to enabling large-scale photonic quantum information processing as compatibility
with CMOS processing provides a demonstrated path to upsizing the number of photonic components\textsuperscript{109}. Another key advantage is the potential to place control electronics on the same chip as the optics. Silicon has been used as the basis for integrated photonic devices to demonstrate quantum key distribution in a range of different experiments\textsuperscript{110}, including real-world implementation\textsuperscript{111}. In these experiments, Silicon photonic circuits allowed the authors to integrate all the functionalities of the transmitter module, apart from the laser, into a single chip suitable for mass production. Both groups use electro-optic absorption modulators to encode quantum information.

Demonstrations of correlated photon pair sources in silicon waveguides are numerous since the first in 2006\textsuperscript{112}, and include devices fabricated with CMOS processes\textsuperscript{113}. There has also been demonstrations of on-chip sources showing quantum interference in silicon\textsuperscript{114}. These remove the necessity for external sources of single photons and are necessary for any large-scale experimental demonstrations. Entanglement, and two qubit processing has been demonstrated on a chip with four integrated sources and a waveguide processing network, in one of the most complex integrated quantum photonic demonstrations to date\textsuperscript{115}. The chip consists of spiral waveguides used as sources of single photons from spontaneous four wave mixing, and thermo-optic phase shifters contained in networks of Mach-Zehnder interferometers to implement arbitrary single qubit rotations a controlled-Z gate, and measurement projection operations. Probabilistic quantum controlled-not gates have also been demonstrated with footprints as small as 196\textmu m\textsuperscript{2}\textsuperscript{,116} and while their performance is not yet suitable for large scale integration, their footprint can already enable production of thousands of quantum logic gates on a single chip, in comparison to a bulk optical setup taking a large portion of an optical table. The largest such demonstration to date integrates sixteen indistinguishable single photon sources and 550 photonic components on a single chip for generation and detection of bipartite entanglement using qudits with dimensionality up to 15\textsuperscript{76}.

Large reconfigurable quantum walk circuits have also been shown on silicon\textsuperscript{117}. Single photon detectors with efficiencies up to 70% have been integrated with silicon waveguides\textsuperscript{118,119}. Homodyne detectors, with a bandwidth of 150MHz, and photodiode quantum efficiency of 64% have been integrated in a silicon platform and
used for random number generation\textsuperscript{120}. There has also been a demonstration of hybrid integration of single emitters into a silicon waveguide\textsuperscript{121}. The lack of a low loss high speed modulator in silicon is a bottleneck in progress towards integrated photonic quantum computation\textsuperscript{84} as will be discussed in 1.4, and many of the advantages of piggybacking on CMOS processes will be lost unless single photon detectors can also be fabricated in a CMOS compatible way.

III-V semiconductors have a considerable processing expertise base from their use in electronics applications. Because of their ease of growth with chemical vapour deposition systems, waveguides in III-V materials are usually made as nanowires on top of a confinement layer made of another, compatible, III-V material usually on top of a III-V wafer. Many of this family of materials offer similar integration densities to silicon and have several material advantages, including the existence of a second-order nonlinearity, telecom wavelength photodiodes, and integration of single photon emitters and detectors. Gallium arsenide has drawn particular attention due to the quality of single emitters available\textsuperscript{122,123}. These single emitters are in the form of a quantum dot created by deposition of an InGaAs layer on top of the GaAs. The highest performance quantum dots have their emission enhanced by a micro-pillar cavity formed by Bragg mirrors. This cavity increases emission brightness in the cavity mode through the Purcell effect with source brightnesses up to 65% demonstrated\textsuperscript{122}. An example schematic is shown in Figure 4.

\begin{figure}[h]
  \centering
  \includegraphics[width=0.5\textwidth]{figure4.png}
  \caption{Schematic of a micro-pillar quantum dot, comprised of top and bottom Bragg mirror layers (usually 20-30) around a quantum dot layer (red), with enhanced emission into the vertical cavity mode.}
\end{figure}

GaAs devices with single qubit operations and on chip quantum interference have been demonstrated using off-chip single photon sources and detectors with an
integrated beamsplitter. Integration of single emitters and beamsplitters has also been achieved in GaAs and InGaAs, including recently, deterministic placement of the single emitters, and high performance single emitters. Single photon detectors have been successfully integrated in GaAs with efficiencies up to 20%, and photon number resolving detectors demonstrated in GaAs/AlGaAs waveguides. It is expected changes in materials used for single photon detectors can improve efficiencies.

GaAs has a large second order nonlinearity, allowing efficient non-linear optical processes. Quasi phase matching has been achieved in GaAs, however it requires specialised crystal growth, rather than wafer-scale processing. Nonetheless, direct phase matching has allowed demonstrations of photon pair, and bell-pair sources in these substrates. While III-V substrates have demonstrated excellent abilities to generate, actively manipulate, and detect quantum states on-chip, the specialised fabrication procedures for each component have not been demonstrated on a single chip, and indeed some of them are incompatible. The first of these more complex integrated systems was demonstrated by Midolo et al. and included a single emitter and an electro-optic router on a single chip. Recently, single photon sources, a beamsplitter, and single photon detectors have been fabricated on a single device, however source and detector performance were not as good as on individually fabricated devices. Whilst III-V semiconductors remain one of the most promising platforms, demonstrations that are more complex will require considerable technological achievements, and large waveguide arrays are yet to be demonstrated.

Lithium niobate is a material with a long history of use in classical integrated optics, and is a core part of modern telecommunication infrastructure. For this reason, it has established fabrication techniques and highly advantageous material properties, which allow it to be used to create a range of components essential to quantum photonics. As with the other materials, there are several distinct ways to create waveguides in lithium niobate. The most generally used is titanium in-diffusion; however, these waveguides have poor confinement and extremely large bending radii, and are more suited to straight-line devices. Recently, ridge waveguides fabricated on thin film lithium niobate on insulator (LNOI) substrates have shown
promising results\textsuperscript{141}, with small device sizes and high nonlinear efficiencies; however, the fabrication knowledge base is not yet fully developed. Additionally LNOI substrates should be more suitable for integration of detectors\textsuperscript{141}. Proton exchange offers an in between point in terms of confinement and device size, with well-known fabrication techniques, and high fabrication yield.

![Image](image_url)

**Figure 5** Periodically poled waveguide used for frequency conversion between UV and telecom wavelengths. Straight waveguide and entire chip is illuminated by the pump wavelength of 482nm necessary for the difference frequency generation with the signal at 369.5nm. Waveguide chip is located in temperature controlled mount and input and output coupling performed by aspheric lenses.

The first quantum optics application of waveguides in lithium niobate was generation entangled photon pairs with higher efficiency than bulk processes\textsuperscript{142–144}, demonstrating the performance advantages of an integrated source. This work has also been extended to the generation of photon triplets\textsuperscript{145,146}, where the efficiency of two cascaded sources was sufficient to generate triplets at a rate of \(~\)2 per hour. Similarly, LN has been used for a range of heralded single photon sources, including a chip with integrated signal and idler separation\textsuperscript{147} and with multiple sources\textsuperscript{148}. A plug-and-play high brightness lithium niobate waveguide source of single photons was demonstrated in a compact and stable package suitable for field-testing of quantum communications systems\textsuperscript{149}. High nonlinear process efficiencies have also meant lithium niobate is the material of choice for wavelength conversions necessary to interface various quantum systems via optical fibre links, which operate most efficiently at telecom wavelengths\textsuperscript{150–153}. An image of the waveguide used for
frequency conversion between a laser at the readout transition of $^{174}\text{Yb}^{+}$ (369.5nm) and telecom wavelengths by Kasture et al.\textsuperscript{154} is shown in Figure 5.

Demonstrations of ultra-broadband spontaneous parametric down conversion\textsuperscript{155} are of interest for generation of entangled frequency combs\textsuperscript{156}, and wideband sources of squeezing. The first integrated source of squeezing was fabricated in an periodically poled lithium niobate waveguide circuit\textsuperscript{157}, with a demonstrated squeezing of 1dB. Coupled waveguide arrays in lithium niobate were among the first experiments across many optical modes, produced simulations of fundamental interest\textsuperscript{158}.

Recent works have shown progression to more complex demonstrations. Martin et al. created a quantum relay chip comprised of pair generation from spontaneous parametric down conversion and two tunable directional couplers\textsuperscript{159}. Zhang et al. showed quantum interference from on-chip generation of spatially separated photon pairs\textsuperscript{160}. Bonneau et al.\textsuperscript{161} showed active manipulation of single photon path and polarisation in lithium niobate to demonstrate on-chip entanglement preparation, tuneable quantum interference, and quantum state engineering. Jin et al.\textsuperscript{162} report on chip generation and manipulation of entangled photon pairs. Solntsev et al. demonstrate non-classical biphoton state generation using a quantum walk through evanescently coupled waveguide array in lithium niobate\textsuperscript{163}.

Commercially available electro-optic modulators rely on integrated optics to enable their high-speed operation. Such modulators have been used to demonstrate fast feedforward operations in quantum optics, as necessary for most computation protocols. Fast feedforward with lithium niobate modulators has been used to demonstrate probabilistic cloning of quantum states with fidelity higher than the deterministic limit\textsuperscript{164}. It has also been used to reduce the noise of quantum state amplification below the deterministic level\textsuperscript{164}. Together with its high nonlinear efficiency, the availability of high performance active components makes lithium niobate an excellent choice for quantum optics, particularly those experiments that require fast reconfigurability. The reconfigurability of integrated optical circuits will be discussed in more detail in section 1.4.

Two key challenges are present for the lithium niobate platform, device size, and incompatibility with growth processes for other materials. Compatibility with other materials is required for integration of detection systems. Studies have looked at
integration of photodiodes\textsuperscript{165,166}, and single photon detectors\textsuperscript{167,168} on lithium niobate substrate with limited success. These integrated photodiodes have absorption coefficients up to $40\text{cm}^{-1}$ but no reported system efficiencies. Single photon detector efficiencies up to 0.15\% have been reported\textsuperscript{168}. Neither of these reported results are suitable yet for quantum optics applications and these results are considerably less advanced than silicon. Nonetheless, the highly advantageous material properties make it worthwhile pursuing these technologies on lithium niobate in parallel with more complex demonstrations using currently available technology.

Table 3 A summary of critical information for each waveguide material platform as applicable to quantum information. Effective refractive index contrast gives an indication of potential device size and density. Remaining fields indicate properties relevant to the generation, active manipulation, feedforward, and single photon detection capabilities of each platform. SFWM – spontaneous four wave mixing, SPDC- spontaneous parametric down conversion, PE – reverse proton exchange

| Waveguide Effective Refractive Index Contrast | Silica/Glass | Silicon | GaAs | LiNbO$_3$
|---|---|---|---|---|
| ~0.4 (Ridge) | ~0.01 (LW) | 2.02-2.48 | 1.92-2.38 | $\sim10^{-3}$ (RPE) $\sim10^{-4}$ (Ti) 0.7-1.1 (Ridge)
| Single photon source | SFWM | SFWM | Quantum Dot, SPDC | SPDC
| Active Element | Thermo-optic (DC-kHz) | Thermo-optic (DC-kHz) | Electro-optic (DC-GHz) | Electro-optic (DC – THz)
| Single photon detector efficiency | 79\% (photon number resolving)\textsuperscript{103} | 91\%\textsuperscript{118} | 47.5±15.7\%\textsuperscript{139} | 0.15\%\textsuperscript{168}
1.3. Nonlinear high-speed reconfigurable integrated photonics in lithium niobate

Lithium niobate is the material that underpins the research presented here, and the fabrication of custom lithium niobate integrated circuits for quantum optics is the primary focus of this work. Lithium niobate has a plethora of advantageous material properties that make it an ideal platform for quantum optics that will be discussed in this section. The general technique for fabrication of nonlinear, electro-optically reconfigurable integrated photonics is also reported here with specific details of each individual device created listed in respective chapters.

Lithium niobate (LN, chemical formula LiNbO$_3$) is a non-centrosymmetric monocrystalline material with a wide bandgap, available in wafers up to 5” in diameter$^{169}$. It has several key properties of significant interest for integrated quantum photonics, namely:

- Wide transparency window (~350nm-4.5\(\mu\)m) suitable for frequency conversion and low propagation loss waveguides.
- High non-linear coefficient (27pm/V) and ferroelectric domains suitable for efficient non-linear optical processes and photon pair generation.
- High electro-optic coefficient (33pm/V) suitable for electronically controlled active optical elements.

To take advantage of these characteristics we fabricate devices using annealed and reverse proton exchange waveguides on 3” 0.5mm thick X and Z-cut LN substrates. In this work we fabricate the photonic switch used for the experiment in chapter 2 using annealed proton exchange on an X-cut substrate. For the optical splitter used in chapter 4, and the CV entangler of chapter 5 we use reverse proton exchange on Z-cut substrates. All fabrication is performed in house at Griffith University between the cleanroom facilities of the Queensland micro-technology facility (QMF) and the state of the art lithium niobate fabrication equipment of the Integrated Quantum Technologies group.

The two crystal cuts both have distinct advantages for specific applications. The extraordinary axis of LN and its largest non-linear and electro-optic coefficients are oriented in the Z direction, meaning Z-cut is the preferred choice for using standard
periodic poling techniques as this creates the periodic poling in the direction with the largest non-linearity. Thus, Z-cut substrates are preferable for non-linear applications. X-cut substrates, unlike Z-cut do not suffer from build-up of surface charges, and are thus easier to use during fabrication, and do not suffer from DC drift when a DC voltage is applied to the wafer, meaning they are preferable for electro-optic applications.

Excellent control is available over the produced structure using reverse proton exchange, with a complete empirical model of our waveguide fabrication described by Lenzini et al.\textsuperscript{170}. Full details of the process are also previously reported\textsuperscript{171}, but for completeness a brief description is shown in Figure 6 and detailed below.

Firstly, a photoresist mask is defined by optical lithography for periodic poling. Periodic poling is the process of creating regions, through which the light will propagate, where there is a regular flipping of the crystal polarisation. Periodic poling enables nonlinear optical processes that would otherwise be forbidden by energy and momentum conservation through a technique known as quasi-phase matching.

Optical fields can be mixed in media with an interaction strength proportional to the nonlinear coefficient. For second order nonlinear media this mixing occurs between three fields. However for this interaction to occur energy and momentum must be conserved in the interaction.

When we wish to mix three fields where momentum conservation would not occur in bulk crystal we must alter the crystal properties. We may describe the momentum of the three fields by their k-vectors, $k_1$, $k_2$, $k_3$, and their conservation by $k_1 + k_2 - k_3 = \Delta k = 0$. If we introduce a structure that periodically inverts the sign of the interacting fields’ momenta each length $\Lambda/2$, we create an effective momentum term $G = \frac{2\pi}{\Lambda}$. When we choose $\Lambda = \frac{2\pi}{\Delta k}$ we remove the momentum mismatch between the propagating fields, and thus the nonlinear process may proceed. This technique is known as quasi-phase matching as phase ($\phi$) and momentum are related by $e^{i\Delta \phi} = e^{i\Delta k z}$. This periodic inversion can be achieved by flipping the sign of the nonlinear coefficient through inverting the crystal’s ferroelectric domains.
Figure 6 Overview of our process flow for fabrication of non-linear, electro-optic, integrated photonic devices in lithium niobate.

The inversion of the ferroelectric domains is done by contacting the wafer with a liquid electrolyte in the gaps of the photoresist mask, and applying a voltage larger than the domain breakdown voltage (21kV/mm) between the two sides of our wafer. The resultant structure can be revealed by piezo-resistance force microscopy or through wet etching with 50% Hydrofluoric acid. HF preferentially attacks the -Z face, causing it to be etched much faster than the +Z face, hence showing the difference in crystal polarisation as shown in Figure 7. The photoresist mask is then removed and the wafer sputter-coated with titanium. This titanium is patterned with photolithography and etching leaving only the regions of the wafer where waveguides are to be formed exposed.

Figure 7 Left shows periodic poling structure for quasi-phase matching. Right shows a 40x microscope image of a part of a fabricated electrode.

Proton exchange is performed by immersing the wafer in pure benzoic acid at 170°C in a temperature stabilised oil reactor. During this process, protons diffuse into the exposed parts of the LN wafer with the process driven by a chemical potential
gradient created by the different hydrogen ion concentrations. To maintain charge neutrality the hydrogen ions that move into the crystal are replaced by lithium ions moving into the benzoic acid\textsuperscript{172}. The proton exchange process creates an increased extraordinary refractive index, and a reduced ordinary refractive index, meaning that light will be guided in only one polarisation.

To increase stability and recover the diminished nonlinear coefficient of the waveguide region a thermal annealing is performed at 328°C in dry atmosphere after the metal mask is removed. During this time, hydrogen ions thermally diffuse further into the substrate creating a waveguide with a gradient refractive index that is stable and with mostly recovered nonlinearity.

Next, the reverse proton exchange process can be used to improve the symmetry of the waveguide mode, its overlap with optical fibre, and its propagation loss. The wafer is immersed in a eutectic melt of lithium nitrate, sodium nitrate, and potassium nitrate also at 328°C\textsuperscript{173}. In this melt, only the hydrogen ions very close to the surface are replaced in the crystal by lithium ions, hence, much of the annealed hydrogen concentration remains in the crystal, buried away from the surface by the re-exchange of lithium, and thus the mode of the waveguide is moved further away from the surface.

![Figure 8 Photographs of finished integrated photonic device in lithium niobate illuminated with red light. Optical coupling can be achieved either from fibre butt coupling or with a lens. Electrical signals are applied to the printed circuit boards via SMA cables from 50Ω sources. The left figure shows testing with electronic probes before printed circuit boards are wire bonded in as shown in the right figure.](image)

22
Finally, a silicon dioxide buffer layer is sputtered over the surface of the wafer, and metal electrodes are patterned onto the buffer layer by sputtering, photolithography, and etching. A close up image of fabricated electrodes is shown in Figure 7. Dicing and polishing of end facets to an optical finish completes the fabrication before electrical contact is made to the electrodes through wire bonding to custom designed circuit boards. An example of a finished device is shown in Figure 8 above.

1.4. **Active integrated quantum photonics**

For a range of quantum communication protocols, discrete variable and continuous variable quantum computation, high-speed reconfigurable photonic circuits are necessary. For quantum communication, reconfigurable optics is necessary for phase, polarisation or amplitude encoding, and the requirement of high bitrate demands encoding happens at high speed. For linear optical quantum computation, low loss high-speed reconfigurability is necessary for implementing feedforward operations quickly\(^{74}\). High-speed reconfigurability is also necessary for multiplexing low brightness sources together to make sources of sufficient brightness to be used in universal quantum computation protocols as discussed in 1.1.1 above. For continuous variable quantum computation, high-speed measurement feedback control is required\(^{73}\), and thus fast reconfigurability is necessary. In each of these cases, faster reconfigurability enables higher communication and source repetition rates, shorter delay lines, and shorter quantum memory storage times enhancing performance.

For quantum communication reconfigurability at similar rates to classical communications i.e. 10-40Gbps, corresponding to modulation frequencies of tens of gigahertz are desirable to increase data rates. For quantum computation, and source multiplexing, system speed should ideally be only limited by detector refresh rate, which depending on the detection system, ranges from \(10^8-10^{10}\)Hz. This means circuit reconfigurability should employ GHz speeds or greater.

For materials lacking second order nonlinearity such as silica, silicon nitride, and silicon, this presents a challenge. All reconfigurable quantum optic circuits to date in these platforms have used thermo-optic phase shifters. These devices take advantage of the thermo-optic effect, whereby a change in temperature causes a change in
refractive index. In silicon this effect is relatively large at room temperature,\textsuperscript{175} with 
\[
\frac{dn_{Si}}{dT} = 1.86 \times 10^{-4} K^{-1},
\]
but in silica it is considerably lower\textsuperscript{176}, 
\[
\frac{dn_{SiO_2}}{dT} = 8.66 \times 10^{-6} K^{-1}.
\]
The fastest thermo-optic phase shifters operate at only 130 kHz and consume 24mW of power for a \(\pi\) phase shift\textsuperscript{177}. This rate imposes a limitation on the overall system rate, especially if reconfiguring is required between every measurement.

As well as being slow, the high power consumption and heating will pose considerable design challenges for large integrated circuits. The heat input at one resistive heater will gradually spread across the thermally conductive substrate; and thus crosstalk between devices becomes a considerable control problem. Additionally, with a moderate size circuit consisting of 1000 phase shifters will already thermally dissipate 24W, a value beyond the cooling power of most cryostats needed to run integrated single photon detectors. Furthermore the magnitude of the thermo-optic effect reduces dramatically with temperature, dropping to \(10^{-8} K^{-1}\) at 5K\textsuperscript{175}, a decrease of more than four orders of magnitude, requiring more temperature change for the same effect, all without heating up the spatially proximate single photon detectors.

High speed modulators have been shown in silicon using the plasma dispersion effect\textsuperscript{178,179}, whereby the carrier concentration is changed to cause a change in refractive index. This effect changes both the real and imaginary parts of the refractive index, modulating phase, but also intensity in an absorptive way. Thus, they are not presently suitable for quantum optics. More promising approaches use strain engineering\textsuperscript{180} or large DC fields\textsuperscript{181} to induce an electro-optic effect in silicon, however these are yet to be demonstrated in a quantum optics context.

For materials with second-order nonlinearity such as III-V semiconductors and lithium niobate the problem is much easier. In these materials, the refractive index can be altered at high speed through the electro-optic effect. The electro-optic effect changes the real component of the refractive index proportional to the applied electric field and the strength of the second order nonlinearity in the medium according to the equation; 
\[
\frac{dn}{dE} = -\frac{1}{2} n^3 \varepsilon_0 E,
\]
where \(\varepsilon_0\) is the electro-optic coefficient in the direction that the electric field \(E\) is pointed.
Figure 9 Simulated electric field for an electro-optic phase modulator, applying +10V to the signal electrode. Substrate is lithium niobate and the red circle indicates the approximate position to place waveguides in X-cut and the white circle for Z-cut. These electrode placements ensure the electric field in the waveguide point in the direction of the largest electro-optic coefficient.

The electro-optic effect has been used to demonstrate low loss modulators with responses up to 1 THz in thin film lithium niobate\textsuperscript{182}, and devices with speeds of 40GHz are in standard use in classical communications systems. As capacitive rather than resistive electrodes supply the required electric field, power dissipation occurs only through leakage paths. An example of the electrode design used to create the required electric field within the waveguide is shown in Figure 9. In lithium niobate the temperature dependence of the electro-optic coefficient has been observed, with the value of the largest coefficient, $r_{33}$, dropping from $31 pm/V$ at room temperature to $24 pm/V$ at 7K\textsuperscript{183}, demonstrating the suitability of electro-optic modulators for cryogenic compatible experiments with single photon detectors.

1.5. Photonic multiplexing for quantum information

Multiplexing is the process of using one resource to overcome the scarcity of another resource. In electronics and classical communications, numerous multiplexing schemes trade-off between limitations to bitrates or number of channels, using space, time, frequency, polarisation, or orbital angular momentum as the plentiful resource. Wavelength division multiplexing is the backbone of fibre-optical communications systems, with many different frequencies transmitted along a single optical fibre, each
carrying information to a separate receiver. This allows bitrates through a single channel a factor of 100 faster than the bandwidth of a single transceiver.

In photonic quantum information experiments, there are several technological bottlenecks due to lack of resource availability as discussed below. This work aims to harness multiplexing to address these shortfalls by utilising other degrees of freedom to improve the performance of critical resources.

In discrete variable quantum computation, arguably the biggest shortage is of indistinguishable single photons. To date there is no bright source of indistinguishable single photons, with the most commonly used sources, namely spontaneous parametric down conversion (SPDC) or spontaneous four wave mixing (SFWM) being intrinsically low brightness to maintain their single photon nature. Thus for parametric down conversion, a minimum of 17 sources will be required to be spatially multiplexed together to create a source with >99% brightness. Numerous experiments have used between two and five spatially multiplexed SPDC or SFWM sources to create between two and ten entangled single photons. However, these experiments do not address the low brightness of each individual source, meaning they are neither experimentally extensible nor theoretically scalable. Most of the initial work in multiplexing single photon sources in integrated optics has been looking at combining many low brightness sources into a single high brightness source as proposed by Migdall et al. In 2011, the first experimental demonstrated spatial multiplexing of four SPDC sources to create one single photon source of high brightness was performed in bulk optics, using electro-optic modulators to multiplex photons into a single spatial mode. The first integrated optic demonstration of photon source multiplexing used a 2x2 lead lanthanum zirconium titanate (PLZT) optical switch. Following demonstrations have used temporal, spatial-temporal,

---

4 The probability for generating a pair of photons is proportional to pump power ($\eta$) and the probability for generating two pairs is proportional to pump power squared, i.e. the output state $|\psi\rangle \propto |0,0\rangle - \eta |1,1\rangle + \eta^2 |2,2\rangle$. Thus, the only way of reliably generating just one pair is to keep the pump power, and thus the generation probability low.

* This scheme also assumes the availability of 100% efficient photon number resolving detectors to post-select on single pair generation events, so the realistic number will be much higher.
and frequency multiplexing in various experimental platforms to increase the brightness of a single photon source\textsuperscript{148,189–195}.

The advent of high brightness micro-pillar quantum dot single emitters\textsuperscript{122,123}, has created an alternative scenario, with the scarce resource instead being number of indistinguishable sources rather than source brightness. Our work presented in Chapter 2, uses multiplexing to redistribute resources advantageously in this scenario.

In continuous variable (CV) quantum computation experiments time and frequency multiplexing are used in the preparation of the cluster state structure. Through the use of an optical frequency comb, sixty simultaneously available entangled modes of a continuous variable cluster state have been generated\textsuperscript{196}. Through temporal-multiplexing, continuous variable cluster states of up to one million modes have been generated\textsuperscript{78}, and arbitrarily large states are possible with the same technique. An experimental proposal also exists for the combined use of frequency and time multiplexing to generate arbitrarily large cluster states\textsuperscript{197}. Following the proposed design of Menicucci\textsuperscript{73} we aim to use temporal multiplexing to create continuous variable cluster states. We implement the first building block, namely a pair of squeezers with high-speed reconfigurable interference. Two of these modules will feed into a nested interferometer delay setup to create a temporally multiplexed CV cluster state. This high-speed reconfigurability will provide more flexibility in the created state by allowing control over the degree of entanglement between cluster state nodes.

In quantum communications experiments, and in particular quantum key distribution (QKD), multiplexing is required to improve single channel transmission rates\textsuperscript{198}, and overcome bitrate limitations of transmitter-receiver pairs\textsuperscript{199}, as well as to provide flexible connectivity\textsuperscript{200}. Current systems are limited to kilobit and megabit\textsuperscript{201,202} data rates, which is not yet sufficient to replace classical communications in all tasks. With increasing communication rates comes a requirement for more random numbers, which are necessary for encryption in all QKD protocols. These random numbers should come from a non-deterministic, i.e. quantum, random number generator to ensure security. It is reasonable that just as the transmitters and receivers of QKD are parallelised to allow multiplexing, the random number generator supplying these
systems should produce parallel streams of random numbers. Furthermore, limitations of processing speed and detection bandwidth restrict random number generation rates. As such spatially multiplexed detection and processing for quantum random number generators can be used to improve their speed and compatibility with QKD. This suggestion has been identified in reviews of quantum random number generation\textsuperscript{203,204}, and experimentally implemented for the first time in work presented in Chapter 4.

1.6. Thesis structure

The next chapters are presented as a series of published and unpublished papers in accordance with Griffith university policy on inclusion of papers within a thesis. Each chapter presents a foreword establishing the link between the included paper and other content of the thesis, as well as the paper itself.

Chapter 2 presents published work regarding the demultiplexing of single photons from a quantum dot\textsuperscript{205}. In this work, we describe the fabrication and operation of an integrated optical switch. We apply this optical switch to the problem of generation of a multi-photon source from a single solid-state quantum emitter.

Chapter 3 presents published work that details an electronic device suitable for delivering many synchronised ±15V pulses at high speed\textsuperscript{206}. In this work, a field programmable gate array is used as a source for many parallel pulse sequences, which are then processed and amplified to form the necessary driving voltage for an optical switch made in lithium niobate as described in chapter two.

Chapter 4 focuses on multiplexed quantum random number generation, including a paper submitted for publication. We create a system for generating random numbers from many parallel homodyne measurements of the quantum vacuum state. We use this new scheme to create the first generator of random numbers that runs at MHz rates whose security is not reliant on any classical process.

Chapter 5 describes the complete integration of a building block needed for time multiplexed continuous variable quantum computation algorithms, and includes a paper submitted for publication. It represents the first demonstration of quantum
light sources, actively reconfigurable photonic circuits, and quantum light detection in a monolithic package.

Finally, some concluding remarks present future directions for quantum optics to use multiplexing to overcome performance issues.
2. Demultiplexing Single Photons

2.1. Statement of contribution to co-authored published paper

This chapter includes a co-authored paper. The bibliographic details of the co-authored paper, including all authors, are:


The integrated optical switch was designed and fabricated by B.H., F.L., and S.K., with wire bonding performed by H.-P.P. Quantum dot fabrication was performed by I.S., A.L. and P.S. with and J.C.L. and N.A.Z characterised its operation. F.L., B.H., J.C.L, and R.A.A. performed experimental measurements. D.V.D, P.S., M.P.A, A.G.W and M.L. supervised the project. F.L, B.H. and M.L prepared the manuscript with contributions from all authors

My contribution to the paper involved:

- With authors 1 and 6, the design and fabrication of the integrated optical switch.
- With authors 1 and 4, test and measurement of the operating conditions of the integrated optical switch.
- With author 3 designing and performing the experimental measurements of single photon demultiplexing
- Data analysis of experimental measurements of single photon demultiplexing
- With all authors writing and editing the manuscript.

(Signed) (Date) 27/07/2018
Benjamin Haylock

(Countersigned) (Date) 27/07/2018
Corresponding author of paper: Mirko Lobino

(Countersigned) (Date) 27/07/2018
Supervisor: Mirko Lobino
2.2. Fully integrated active optical demultiplexer

It is natural that as the field of quantum physics has moved from demonstration towards application that protocols using single photons have remained at the forefront of efforts to build quantum computers and long distance quantum communication networks. However, this push for expansion in the size and complexity of systems has encountered several bottlenecks. Of those that remain unsolved, the ability to generate large numbers of indistinguishable single photons is arguably the most pressing. Efficient detection has been demonstrated, but the largest quantum optical demonstrations still rely on inextensible technology to create single photons\textsuperscript{185}.

Spontaneous parametric down-conversion (SPDC) and spontaneous four wave mixing (SFWM) are still the primarily used sources; however, they are intrinsically non-deterministic, meaning protocols cannot be effectively scaled. The generation probability of a photon pair must remain low to ensure the probability of the unwanted photon number components of SPDC and SFWM, i.e. higher order terms, remain insignificant. For most quantum computational applications many photons are required, and thus many independent sources. As the probability of getting photons from all sources simultaneously is equal to the product of each individual source probability, when individual source probabilities are low, many-photon rates limit experimental complexity.

To address this shortcoming there has been an entire field of work to generate single photons through other methods. Quantum dots have been studied as sources of single photons, with their artificial atomic properties making them high purity sources of single photons. By embedding such dots into micro-fabricated optical pillar cavities, pumping and collection efficiencies can be greatly improved, offering sources with brightness up to three orders of magnitude higher than equivalent SPDC sources\textsuperscript{122}.

A considerable drawback of these micro-pillar quantum dots is that different devices, fabricated to be identical, remain distinguishable, preventing the fabrication of many to each act a single photon source. Together with a high-speed reconfigurable optical circuit, we can use a single quantum dot to create a multi-photon source through spatial demultiplexing.
This work came about through previous work in the group of Andrew White at the University of Queensland. They have installed and characterised micro-pillar quantum dots fabricated in the group of Pascale Senellart at Université Paris-Saclay. They performed measurements of the indistinguishability of consecutively emitted photons from the installed quantum dot, and realised its potential to generate multiphoton Fock states through temporal multiplexing\(^{207}\). They first used a passive multiplexing scheme, consisting of two beamsplitters to perform high-speed three photon boson sampling\(^{208}\). However they found passive multiplexing is not suitable as its efficiency drops as \(n^{-n}\), where \(n\) is the number of photons. The proposed solution was high speed active multiplexing, for which our group could create the necessary technology using waveguides in lithium niobate. This led to the experiment as described below.

2.2.1. Included Paper - Active demultiplexing of single photons from a solid-state source

*The remainder of this page is intentionally left blank.*
Abstract

A scheme for active temporal-to-spatial demultiplexing of single photons generated by a solid-state source is introduced. The scheme scales quasi-polynomially with photon number, providing a viable technological path for routing $n$ photons in the one temporal stream from a single emitter to $n$ different spatial modes. Active demultiplexing is demonstrated using a state-of-the-art photon source—a quantum-dot deterministically coupled to a micropillar cavity—and a custom-built demultiplexer—a network of electro-optically reconfigurable waveguides monolithically integrated in a lithium niobate chip. The measured demultiplexer performance can enable a six-photon rate three orders of magnitude higher than the equivalent heralded SPDC source, providing a platform for intermediate quantum computation protocols.

Active demultiplexing of single photons from a solid-state source

Francesco Lenzini¹, Ben Haylock¹, Juan C. Loredo²,³, Raphael A. Abrahão², Nor A. Zakaria², Sachin Kasture¹, Isabelle Sagnes³, Aristide Lemaitre³, Hoang-Phuong Phan⁴, Dzung Viet Dao⁴,⁵, Pascale Senellart³,⁶, Marcelo P. Almeida², Andrew G. White², and Mirko Lobino¹,⁴,*

A key requirement for large-scale quantum photonic technologies is the availability of reliable sources of multiple indistinguishable single-photons. To date, spontaneous parametric down-conversion (SPDC) sources have been the most widely-used technology in the generation of indistinguishable single-photons. However, the presence of unwanted multiple-photon terms in the SPDC state limits the brightness of high-purity single-photon sources to values lower than 1% [1]. To circumvent this limitation different approaches have been introduced, including active spatial [2, 3], temporal [4, 5], and spatio-temporal [6, 7] multiplexing schemes that combine the outputs of many SPDC sources to create one bright source without deteriorating single-photon purity or indistinguishability [5]—although typically at the cost of a large resource overhead in terms of active optical circuits and single photon detectors since a $n$-photon heralded SPDC multiplexed source requires $n$ nonlinear crystals and $n$ single-photon detectors.

In comparison, single emitters have the advantage of producing nearly-pure single-photon Fock states. Very recent advances in quantum dot (QD) technologies have resulted in single-photons sources with simultaneously near-perfect purity, near-unity indistinguishability, and high efficiencies [8, 9]—over an order of magnitude brighter than SPDC sources with equivalent levels of purity and indistinguishability. Thus, quantum dots have now become an attractive platform to develop multi-fold single-photon (multi-photon) sources.

Achieving high indistinguishability and brightness with multiple independent QDs is still a challenge. However, it has been shown that a single QD coupled to a micropillar cavity can emit photons with excellent indistinguishability over long emission timescales [10, 11], meaning that temporal-to-spatial demultiplexing can be used to obtain multi-photon sources. In this work, we implement two important advances towards the realisation of a scalable multi-fold single-photon source. We first demonstrate the active temporal-to-spatial demultiplexing of a stream of photons to create multi-photon sources with small resource overhead. Secondly, we introduce an integrated zero-buffer active spatial and temporal photonic demultiplexing device, suitable for use with high brightness solid-state sources operating at 932 nm.

Figure 1 schematically depicts our proposed demultiplexing protocol. A temporal stream of single-photons emitted from a quantum dot-micropillar system is actively
routed into different spatial channels by an optical demultiplexer. The demultiplexer is an integrated waveguide device with one input and four output channels made of a network of electro-optically reconfigurable directional couplers fabricated on an X-cut lithium niobate substrate by the annealed proton exchange technique [12]. Electrodes are patterned on top of the waveguides as shown in the inset of Fig. 1, and can be used to tune the splitting ratio in the full 0—100% range by changing the phase mismatch \( \Delta \beta \) between interacting modes [13]. Monolithic integration of the directional coupler network on a single chip is necessary for reduced insertion losses, and with our technology it allows up to 10 output channels in a 5 cm long device.

The \( n \)-photon count rate \( c_{DM}(n) \) measured at the output of an \( n \)-channel demultiplexer can be expressed as

\[
c_{DM}(n) = R [\eta_{SD} \eta_{det}]^n S_{DM}(n),
\]

where \( \eta_{SD} = \eta_{QD} \eta_T \) is the product of the source brightness \( \eta_{QD} \), defined as the probability of emitting one photon at the input of the demultiplexer for each excitation pulse, times the total transmission of the device \( T \). \( R \) is the pump rate of the source and \( \eta_{det} \) is the detectors efficiency. \( S_{DM}(n) \) is a parameter which accounts for how the efficiency of the demultiplying scheme scales with increasing number of photons and it represents the limit of what can be achieved by the demultiplexer with a lossless and deterministic source. Note that the term \( [\eta_{SD} \eta_{det}]^n \) is intrinsically probabilistic, and will unavoidably result in an exponential decay with photon number. In a probabilistic scheme [14]—made of a network of passive beam splitters—the demultiplexing parameter scales as \( S_{DM}(n) = (1/n)^n \), super-exponentially decreasing with \( n \)—a non-scalable approach. In contrast, in an active demultiplexing scheme the scaling is

\[
S_{DM}(n) = \frac{1}{n} \left[ \eta_{DM} + (n - 1) \left( \frac{1 - \eta_{DM}}{n - 1} \right) \right],
\]

where \( \eta_{DM} \) is the “switching efficiency”, defined as the average probability of routing a single photon in the desired channel in each time bin. In the limit of deterministic demultiplexing, i.e. \( \eta_{DM} \to 1 \), the scaling becomes polynomial in \( n \)—thus constituting a scalable approach.

The waveguides were fabricated with a 6 \( \mu \)m channel width and a proton exchange depth of 0.47 \( \mu \)m followed by annealing in air at 328 \(^\circ\)C for 15 h. These parameters are chosen in order to ensure good overlap with single-mode fiber and single-mode operation at \( \sim 930 \) nm, the emission wavelength of our InGaAs QD. Each directional coupler has a distance between waveguide centres of 8.8 \( \mu \)m and a 4.5 mm length (equal to three coupling lengths), resulting in complete transmission of light into the coupled waveguide when no voltage to the corresponding switching electrodes is applied. Difference from this ideal behaviour is from non-uniform waveguide channel widths, caused by the resolution of the photolithography.

The performance of the demultiplexer is tested in conjunction with a single-photon source based on a QD deterministically coupled to a micropillar cavity [10, 15]. The experimental setup is schematically shown in Fig. 2a: the QD is quasi-resonantly pumped via p-shell excitation with a 905 nm, 80 MHz, 5 ps pulsed Ti:Sapphire laser. The single-photons have a 932 nm emission wavelength and are separated from the pump beam via a dichroic mirror and a 0.85 nm FWHM bandpass filter. Quarter- and half-wave plates are used at the input for polarisation alignment as the waveguides within the demultiplexer guide one (horizontal) polarisation. In our case, this reduces the available photon flux at the input of the demultiplexer by \( \sim 50\% \) since the source is only weakly polarised [15], an issue absent if operated with sources engineered to exhibit a large degree of polarization. Photons are injected at the input of the device with a lens of NA = 0.55 and all four outputs are collected with a fibre V-Groove array. Photon-coincidences between the output channels are measured using avalanche photodiodes with 30% average quantum efficiency, and a time-tagging module (TTM). The electrodes of the demultiplexer are driven with a custom-made pulse generator based on a field programmable gate array (FPGA) [16]. The FPGA produces a preset sequence of pulses with varying amplitude voltages that are used to tune the splitting ratio of the directional couplers between on and off values. The driving pulses are synchronized with the clock signal of the Ti:Sapphire laser using internal phase-locked loops (PLL) of the FPGA which provide an adjustable time delay with a low time jitter (300 ps) [16]. The demultiplexer can be actively driven into any configuration by changing the programming of the pulse generator, however as the clocking is derived from the pump laser and not the single photon emission it is not an event-ready reconfiguration. Driving voltages were optimized by maximizing the
coincidence counts between the different channels. A non-zero switching voltage is necessary to compensate for fabrication imperfections.

To verify the correct operation of the switches, as well as their synchronization with the master laser, we first reconstruct the time histograms of two-photon coincidences counts between the first output of the demultiplexer and all other channels. The device is cyclically operated such that the first photon is sent to output one, the second to output two, and so on, and coincidences are measured between all four outputs simultaneously. Figure 2b shows the three time histograms (from a total of six pairwise combinations) of the coincidences measured by all four detectors. We observe enhanced peaks in coincidences at the corresponding delays of our demultiplexer, together with suppressed counts at different delays—showing the correct functioning of our device. The non-vanishing coincidence counts (smaller peaks) in the histograms arise from imperfect operation of the modulated couplers. From the data in Fig. 2b we calculated the splitting ratios of the three switches for both settings using a least-squares fitting procedure (see Table 1). The presence of non-zero off values and non-unity on values reveals the non-ideal operation of the device. The absence of counts at zero time delay (at the same level of accidental counts) is due to the low $g^2(0)$ value of the source, measured as $g^2(0) = 0.029 \pm 0.001$ at $P = 3P_0$ in [10].

The Inset of Fig. 3 shows the measured power-dependent rate of two-photon coincidences $c_{\text{DM}}(2)$ at outputs 1 and 2 of our demultiplexer. As expected for a QD pumped under quasi-resonant excitation it follows a saturation function $c_{\text{DM}}(2) = c_{\text{max}}(2)[1 - \exp(-P/P_0)]^2$ quadratic in the $P$-dependence of the single-photon brightness. A fit to the data results in $c_{\text{max}}(2) = 70.9 \pm 3.0 \text{ Hz}$, the maximum detected 2-photon rate, and $P_0 = 348 \pm 16 \mu\text{W}$ the saturation power. We measured two-fold and three-fold photon coincidence rates of $65 \pm 10$ s$^{-1}$ and $0.11 \pm 0.02$ s$^{-1}$ at the output for a pump power $P = 660 \mu\text{W}$. The switching efficiency $\eta_{\text{DM}}$ is finally estimated by fitting all ten combinations of two and three photon coincidence rates with Eq. 1, with $R = 80 \text{ MHz}$, $\eta_{\text{det}} = 30\%$, and $\eta_{\text{SD}} = 0.76\%$ is calculated from the total

<table>
<thead>
<tr>
<th>switch</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>0.87 ± 0.06</td>
<td>0.94 ± 0.05</td>
<td>0.90 ± 0.06</td>
</tr>
<tr>
<td>off</td>
<td>0.06 ± 0.02</td>
<td>0.13 ± 0.03</td>
<td>0.13 ± 0.05</td>
</tr>
</tbody>
</table>

Table 1 Splitting ratios of the directional couplers calculated from the data in Fig. 2b., with uncertainty from the fit confidence. Non-zero off values are caused by incorrect voltages from the pulse generator. Non-unity on values are caused by incorrect driving voltages and deviations from the desired coupling rate due to waveguide imperfections.
number of counts measured with the four detectors. We find an average switching efficiency $\eta_{DM} = 0.78 \pm 0.06$, in good agreement with the value $\eta_{DM} = 0.80 \pm 0.09$ predicted from the measured splitting ratios.

Four-fold coincidences were predicted to be 0.18–0.06 mHz due to the low value of $T$ in the current system, producing insufficient statistics in the acquisition time of 87 min. Dark counts of our detectors were $\sim 300$ Hz per detector, giving no significant contribution to coincidence measurements.

To investigate the potential of our technology for the realisation of a multi-photon source with larger numbers we calculate the expected photon rates at the output of the demultiplexer for a state-of-the-art QD with 15% polarised brightness pumped under resonant-excitation [8]. The total transmission of our demultiplexer is tested by coupling the waveguide with a gaussian mode from a single-mode optical fibre and is found to be $T = 30\%$. This value is compatible with an overlap with the waveguide mode $\simeq 85\%$, as measured from mode imaging at the output of the waveguide. 14% Fresnel losses at the input and output facets and propagation losses $\simeq 0.65$ dB/cm and is the same value measured from a straight waveguide fabricated on the same chip, meaning that the couplers and electrodes did not introduce extra losses. In Fig. 3 we report the expected photon rates for increasing photon numbers calculated for a pump rate $R = 80$ MHz, $\eta_{DM} = 78\%$, and a transmission $T = 0.3/(0.86 \times 0.86)$ corrected for Fresnel losses, that can be eliminated with an anti-reflection coating at the input and output facets. The QD brightness is corrected by an additional loss factor 65% that takes into account the coupling efficiency of the QD emission mode to a single-mode fibre [10]. The proposed system with these parameters is expected to outperform a probabilistic demultiplexing scheme—made of a network of passive beam splitters with zero propagation losses— for a number of photons $n > 4$ and would enable a 6-photon rate $\simeq 0.01$ Hz, which is three orders of magnitude larger than what could be obtained with six heralded SPDC sources with equivalent quality and brightness of 0.075 [8] (see Fig. 3). The same calculation for a resonantly-excited QD with 14% brightness measured at the output of a single-mode fibre [9], would enable, instead, a 6-photon rate $\simeq 0.1$ Hz. This technology offers great potential for further improvement, in particular by the use of the Reverse Proton exchange technique [12] for an improved coupling with optical fibres and reduced surface-scattering losses we estimate that we can achieve insertion losses lower than 3 dB. Furthermore the switching efficiency of the couplers can be increased with an optimized driving voltage and waveguide fabrication process. Such upgrades will enable the scaling of this platform to a larger number of photons.

In conclusion, we have proposed and experimentally implemented an example of active demultiplexing with a single integrated device of single-photons from a solid-state source. The performance of the demultiplexer has been analysed in conjunction with a QD pumped under quasi-resonant excitation and we have discussed the potential of our technology for state-of-the-art quantum dots. The proposed demultiplexing device is of general interest for any bright temporally distributed single-photon source and provides a scalable approach for the realisation of multi-photon sources of larger photon numbers. Our platform thus constitutes a very promising approach for scalable quantum photonics, in particular for protocols of intermediate—i.e., non universal—quantum computation, such as Boson Sampling [17–19], where, arguably, as few as seven photons from an actively demultiplexed quantum dot-based source could finally demonstrate the quantum advantage over classical systems [20].

Acknowledgements. This work has been supported by the Australian Research Council (ARC) under the Grant No. DP140100808 and fellowship DE120101899, the Centre of Excellence for Engineered Quantum Systems (EQUSS: CE110001013) and Quantum Computing and Communication Technology (CQCT: CE110001027), and the Griffith University Research Infrastructure Program. BH acknowledges support through an Australian Government Research Training Program Scholarship. This work was partially supported by the ERC Starting Grant No. 277885 QD-CQED, the French Agence Nationale pour la Recherche (grant ANR DELIGHT), the French RENATECH network and a public grant overseen by the French National Research Agency (ANR) as part of the Investissements d’Avenir program (Labex NanoSaclay, reference: ANR-10-LABX-0035). This work was performed in part at the Queensland node of the Australian National Fabrication Facility.

Received: 6 November 2016, Revised: 9 March 2017, Accepted: 16 March 2017
Published online: 10 April 2017

Key words: integrated optics, quantum optics, quantum dot, single photon.

References


3. Fast Switching Electronics

3.1. Statement of contribution to co-authored published paper

This chapter includes a co-authored paper. The bibliographic details of the co-authored paper, including all authors, are:


B.H. F.L. S.K. and M.L. designed the system, B.H. and P.F. constructed custom electronics, with B.H. performing assembly, programming, and testing under the supervision of E.W.S and M.L. The manuscript was prepared by B.H. and M.L. with contribution from all authors.

My contribution to the paper involved:

With authors 2, 3 and 6, review of existing literature and devices with similar capabilities and their suitability for this new application.

Design of electronic circuitry

- With author 4, production of custom electronic circuit boards
- Design and implementation of field programmable gate array (FPGA) programme
- Test and measurement to obtain experimental results, including data analysis and processing.
- Preparation of figures for manuscript.
- With all authors, preparation of manuscript.

(Signed) (Date) 27/07/2018

Corresponding Author: Benjamin Haylock

(Countersigned) (Date) 27/07/2018

Corresponding author of paper: Benjamin Haylock

(Countersigned) (Date) 27/07/2018

Supervisor: Mirko Lobino
3.2. High speed arbitrary pulsed control sequences

As briefly discussed in 2.2.1 electro-optic control of an integrated optical switch must be achievable in a synchronous manner with other parts of the system, particular the repetition rate of any pulsed input. It was with this purpose in mind that we devised the electronic control system described in 3.2.1 below. Commercial solutions to creating the same control system are prohibitively expensive, starting at around $50-80000 for an incomplete package, requiring extra expenditure for amplification. These systems are overkill for our application as they enable arbitrary waveform generation, when our system requires adjustable voltage arbitrary bipolar pulse sequence generation, a much simpler problem. Field programmable gate arrays (FPGAs) are a very cheap source of many arbitrary pulse sequences. Using an FPGA, 180° power combiners, and amplifiers, we create the pulse sequences we need for less than $4000 in components.

The application of the system is more general than our specific choice, being suitable for any electro-optic system requiring synchronisation with a pulsed laser, and indeed any other application calling for many channels of high voltage, high repetition rate, bipolar, electronic pulses. With this experiment we show that all the required control to extend single photon source demultiplexing to many channels now exists.

3.2.1. Included Paper - Nine channel mid-power bipolar pulse generator based on a field programmable gate array

The remainder of this page is intentionally left blank.
Nine-channel mid-power bipolar pulse generator based on a field programmable gate array

Ben Haylock,1,2,a) Francesco Lenzini,1,2 Sachin Kasture,1,2 Paul Fisher,1,2 Erik W. Streed,1,3 and Mirko Lobino1,2
1Centre for Quantum Dynamics, Griffith University, Brisbane, Australia
2Queensland Micro and Nanotechnology Centre, Griffith University, Brisbane, Australia
3Institute for Glycomics, Griffith University, Gold Coast, Australia

(Received 1 April 2016; accepted 1 May 2016; published online 16 May 2016)

Many channel arbitrary pulse sequence generation is required for the electro-optic reconfiguration of optical waveguide networks in Lithium Niobate. Here we describe a scalable solution to the requirement for mid-power bipolar parallel outputs, based on pulse patterns generated by an externally clocked field programmable gate array. Positive and negative pulses can be generated at repetition rates up to 80 MHz with pulse width adjustable in increments of 1.6 ns across nine independent outputs. Each channel can provide 1.5 W of RF power and can be synchronised with the operation of other components in an optical network such as light sources and detectors through an external clock with adjustable delay. Published by AIP Publishing. [http://dx.doi.org/10.1063/1.4949508]

I. INTRODUCTION

High speed pulse pattern generators are crucial electronics in many experiments including pump-probe systems,1 optical and electronic modulations, and electronic testing. Electro-optically reconfigurable optical networks are used for fast light manipulation in optical communication2 and quantum optics3–5 applications. In particular, large reconfigurable optical networks over multiple spatial modes require the use of several high speed electro-optically reconfigurable devices which need to be driven by synchronised many channel bipolar pulse patterns.

Commercially available pulse pattern generators are generally either inflexible or very expensive per channel, making the cost of driving more than four independent electro-optic devices infeasible. Our design, initially intended for driving a waveguide network of electro-optic switches in Lithium Niobate,6 offers a low-cost, flexible platform capable of delivering nine high speed, 1.5 W pulse patterns. We expect the versatility of the device to allow adaptation for other experiments.

Our key design parameters were as follows:

1. 10-80 MHz bipolar pulses,
2. 3.5–12.5 ns adjustable pulse width with step size of 1.6 ns,
3. nine synchronised channels,
4. variable power output from 10 mW to 1.5 W, and
5. external clocking with controlled delay.

Rectangular pulses are required by our application with adjustable pulse width to suit the specific pulsed master laser used for the electro-optic switches. We require independently variable positive and negative voltages of greater than 10 V to ground across a 50 Ω resistive load in each channel to maximise the performance of the electro-optic switches by compensating for fabrication imperfections. Finally an external clock input with a delay adjustable over at least one clock cycle enables us to synchronise the driving pulses with components external to the waveguide network such as the repetition rate of a master laser. As this electro-optic switch works with a sub-nanosecond pulsed laser system, the waveform of the pulse generator during the off time of the pulse does not affect the performance during the on time of the laser. Many commercial and previously published designs1,7–9 offer several of the required parameters, but none so far offer all five in a single device. Here we report on a design that satisfies all requirements based on a field programmable gate array (FPGA), using the reprogrammable memory and clock control available in such devices.

II. PULSE PATTERN GENERATION

The pulse pattern generation consists of two parts: an FPGA generates a synchronized train of 2.5 V TTL pulses that are subsequently amplified and/or inverted. The components incorporated in the FPGA and used for our application include static random access memory (SRAM) cells, reconfigurable logic elements (LEs), and phase-locked loops (PLLs) for complete clock control. Figure 1 shows the scheme we use for arbitrary pulse pattern generation programmed into a Cyclone III FPGA starter kit from Altera. The external clock is passed into a PLL which generates the output frequency required to clock the memory. The PLL also allows for a variable delay as required to synchronise output pulses with the external system. This clock is passed into a count-up counter to cycle through addresses of the on-chip memory. An M9K on-chip memory receives data for initialisation via USB connection to PC. The resultant outputs from this FPGA configuration are 2N intermediate channels consisting of arbitrary digital pulse patterns. In our scheme, 2N intermediate channels are necessary for N final outputs as the positive and negative pulses in each output are created by one intermediate channel apiece. In our implementation,
we create 18 synchronised intermediate channels to deliver nine outputs. This configuration can be programmed into a connected flash memory to initialise on device start-up, or can be reprogrammed from a connected computer. Clocking the memory at multiples of the required frequency allows for variable duty cycles; however, due to speed limitations of this device, it is not feasible to clock the memory above 640 MHz, limiting the step size of the pulse width to 1.6 ns.

After TTL pulses are generated from the FPGA board, bipolar amplified pulses are generated using the circuit shown in Figure 2(a). Each intermediate channel connects to a 10-2500 MHz manually variable attenuator composed of LAT-12+ (DC-2.5 GHz, 12 dB) and RVA-2500 + attenuators (both Minicircuits) before being combined using a 180° two-way combiner (ZFSCJ-2-1+, Minicircuits, 1-500 MHz). The RVA-2500+ is a voltage variable attenuator which has a bandwidth of 10-2500 MHz, which limits the maximum pulse width of the device to 50 ns. The control voltage to the attenuator is manually tuned using a potentiometer in a voltage divider. The 180° two-way combiner inverts one of the pulse trains creating a bipolar pulse train at the output. These pulses are amplified using a 32 dB, 1-500 MHz, 1.5 W linear amplifier, chosen as it is the least expensive option to meet the key design parameters. We were not limited by the amplifier noise figure in this application. Figure 2(b) shows the measured bandwidth limitation of the amplifier with a full range positive to negative transition taking 0.4 ns longer in comparison to the unamplified pulse. Nine independent synchronised outputs are implemented in our design. This system could be scaled up to 36 outputs with the current FPGA board. The modular nature of this design, with all components connected via SMA cables, enables easy upgrade or replacement of individual components, allowing versatility in the final key requirements of the pulse pattern. All software and circuit designs are available online.

Using this scheme, we created positive and negative pulses with pulse widths ranging from 3.5 ns to 12.5 ns. The minimum width is limited by the speed of the FPGA and the undriven response time of the amplifier. We show this duty cycle range across seven of the parallel output channels simultaneously. Measurements are shown in Figure 3 and they are taken using a Tektronix MSO5204 oscilloscope with a 50 Ω termination. With 50 Ω termination the oscilloscope has a measurement range of ±5 V, and as such each channel is attenuated by 12 dB to allow for measurement, with the amplitude of the measured voltage subsequently rescaled. As our oscilloscope has only four channels, the measurements are taken with a common trigger, and the timing calibrated between separate measurements.

We next establish the core working principle of the device, which is the ability to create many independent synchronised outputs. We demonstrate synchronisation by having two positive pulses common between all nine channels. Independent waveforms in each channel are demonstrated by having two positive pulses common between all nine channels. 

FIG. 1. Components utilised in the Altera Cyclone III FPGA to create a reprogrammable pattern pulse generator. M9K—internal memory of the FPGA board, PR—phase adjustment relative to external clock, EXT CLK—external clock source, CTRL—green control bus from counter for addressing memory. Red lines indicate clock lines, and blue are intermediate channel pulse patterns which are registered at the output of the memory device. The length of the pulse train is limited to the memory depth which can reach 28 kbits for 18 intermediate channels, equivalent to a maximum sequence length of 350 μs at a clock rate of 80 MHz.

FIG. 2. Schematic (a) of the electronics required for the amplification and/or inversion of each output channel. Two signals from the FPGA are individually attenuated and combined before being amplified to create a single bipolar output. VATT—variable attenuator, 2WC—two-way combiner. (b) Measured response of the signal at the input (blue) and output (dotted red) of the amplifier showing the transition time limitation imposed by the amplifier.

FIG. 3. One positive and one negative pulse spaced by 12.5 ns, with pulse widths ranging from 3.5 ns to 12.5 ns, and each measurement taken on a different channel. Displayed pulse sequence repeats at t = 25 ns given a sustained clock input.
the 180° combiner but before amplification. This test sequence involves \( 6.25 \pm 0.3 \) ns pulses with a minimum repetition time of \( 12.5 \) ns. Figure 4(b) shows the amplified output pulses, displaying the distortion of the pulses due to the bandwidth of the amplifier. These independent pulse trains are synchronous to within \( 1.2 \) ns. This range in pulse widths is larger than the phase jitter, which for all outputs is less than \( 300 \) ps peak to peak. The remainder of the asynchronicity is caused by different delay times through both the FPGA to attenuator connections and the amplifier itself, with the pre-amplification pulses having a temporal spread of up to \( 0.6 \) ns. This level of synchronization is sufficient for our current requirements; however, if necessary the delays could be compensated by adding a digital delay line or specific length of cable between the 180° two-way combiner and the amplifier.

III. IMPROVEMENTS AND CONCLUSION

Several changes or upgrades can be implemented in the proposed design for specific applications. If design flexibility is not required, the current system can be integrated onto a PCB using surface mount components by replacing the present amplifier. Using a system mount implementation, the timing mismatch between channels could be reduced by matching track lengths. Suitable amplifier replacement can be made by Gallium Nitride amplifiers (e.g., NPA1003, Macom, 5 W 20-1500 MHz) for achieving a higher speed and a higher power in a cost effective manner. Pulse amplifiers (e.g., NPT2019, Macom, 25 W DC-6 GHz) also offer a cost effective alternative with better pulse shape. Upgrading to a higher speed FPGA will allow increases in the resolution in adjusting the pulse width and inter-channel delay, as internal processes can be clocked much faster. Furthermore, output serialisation, available in many higher specification FPGAs, can be used to multiplex together many memory devices to increase the output pulse pattern rate without an increase in the speed of the logic or memory used.\(^1\) Currently reconfiguration occurs via reprogramming of the FPGA, which could be improved by changing the contents of the memory cells via an available high speed write input.

In summary we have demonstrated a 1.5 W nine channel synchronised pattern pulse generator capable of a pulse repetition rate of 80 MHz with an adjustable pulse width. The mid-range power and external clocking allow for its use as a driver for electro-optically controlled devices for reconfigurable linear optical networks. Importantly the scalability and modular nature of the design creates an adaptable platform for other applications requiring high speed synchronised pulse patterns.

ACKNOWLEDGMENTS

This work has been supported by the Australian Research Council (ARC) under the Grant No. DP140100808. M.L. acknowledges the support of the ARC-Decra No. DE130100304. E.W.S. acknowledges support from ARC-Future Fellowship No. FT130100472. This work was performed in part at the Griffith node of the Australian National Fabrication Facility. A company was established under the National Collaborative Research Infrastructure Strategy to provide nano- and microfabrication facilities for Australia’s researchers. We acknowledge Stefan Morley for his support and assistance in PCB design and manufacture.


\(^10\)See http://www.ebay.com/itm/181777706918 for 1 MHz to 500 MHz 1.5 W HF FM VHF UHF RF Power Amplifier for ham radio with Heatsink.

\(^11\)See https://github.com/bhaylock/9ch-fpga-pulsegen for information about system implementation as well as FPGA and printed circuit board design files.
4. Multiplexed QRNG

4.1. Statement of contribution to co-authored published Paper

This chapter includes a co-authored paper. The status of the co-authored paper, including all authors, is:


C.W. and M.L. devised the experiment. B.H. and F.L. fabricated the waveguide device. B.H. and D.P. designed and implemented the measurements. Randomness extraction techniques were chosen by B.H. and the manuscript was prepared by B.H. and D.P. with contributions from all authors.

My contribution to the paper involved:

- With authors 3 and 5, design of the integrated waveguide network
- Fabrication of the waveguide network
- Design of the measurement and processing electronics
- Conception of the two-source randomness extractor sub-experiment
- With author 2, programming of the FPGA, collection of experimental data, and data processing and analysis, preparation of figures
- With all authors, manuscript preparation.

(Signed) (Date) 27/07/2018
Benjamin Haylock

(Countersigned) (Date) 27/07/2018
Corresponding author of paper: Mirko Lobino

(Countersigned) (Date) 27/07/2018
Supervisor: Mirko Lobino
4.2. Multiplexed quantum random number generation

True randomness, as generated from quantum processes, is essential for quantum communication and cryptography. It is also a high quality source of randomness as needed for non-security related applications such as Monte-Carlo simulation, gaming, and gambling. Randomness sources for classical communications are not sufficient for quantum cryptography, as the randomness generation becomes a significant security loophole. Currently real-time quantum random number generation rates available are not sufficient for high bandwidth, high speed communication, but instead are useful for security key distribution only.

While the idea of multiplexing the number of channels in a quantum random number generator has been recently published in a couple of reviews\textsuperscript{203,209}, our first introduction to the idea came from Christian Weedbrook, CEO of Xanadu, a quantum computing start-up. He presented to us the idea of using multiplexing to create an ultrafast quantum random number generator, and we completed fabrication of a device, and a proof of principle experiment to show the versatility of the scheme. The key motivation behind this was to create a quantum random number generation architecture suitable for large volumes of network traffic, rather than most current technologies that are suitable for encryption of small volumes of highly sensitive information. We use a large integrated network of 31 beamsplitters to multiplex the generation of quantum random numbers. Creating the same experimental setup in free space would be expensive, cumbersome, and difficult. We show that integrated photonics offers extensibility in quantum cryptography through the potential for increasing quantum random number generation rates.

4.2.1. Included Paper - Multiplexed quantum random number generation

The remainder of this page is intentionally left blank.
Multiplexed quantum random number generation

Ben Haylock1,*, Daniel Peace1,*, Francesco Lenzini1, Christian Weedbrook2 and Mirko Lobino1,3,#

1Centre for Quantum Dynamics, Griffith University, 170 Kessels Rd, Nathan, Queensland, Australia
2Xanadu, 372 Richmond St W. Toronto, Ontario, M5V 2L7, Canada
3Queensland Micro and Nanotechnology Centre, Griffith University, 170 Kessels Rd, Nathan, Queensland, Australia
*These authors contributed equally to this work.
#Corresponding author: m.lobino@griffith.edu.au

Abstract: Fast secure random number generation is essential for high-speed encrypted communication, and is the backbone of information security. Generation of truly random numbers depends on the intrinsic randomness of the process used and is usually limited by electronic bandwidth and signal processing data rates. Here we use a multiplexing scheme to create a fast quantum random number generator structurally tailored to encryption for distributed computing, and high bit-rate data transfer. We use vacuum fluctuations measured by seven homodyne detectors as quantum randomness sources, multiplexed using a single integrated optical device. We obtain a random number generation rate of 3.08 Gbit/s, from only 27.5 MHz of sampled detector bandwidth. Furthermore, we take advantage of the multiplexed nature of our system to demonstrate an unseeded strong extractor with a generation rate of 26 Mbit/s.

© 2018 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

OCIS codes: (270.5568) Quantum Cryptography; (270.5565) Quantum Communications; (130.3730) Lithium Niobate.

References and links

7. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. 221, 1–30 (2016).
Information security [1] is a foundation of modern infrastructure with quantum optics set to play a prevalent role in the next generation of cryptographic hardware [2]. Randomness is a core resource for cryptography and considerable effort has gone into making systems suitable for supplying high bit rate streams of random bits. The randomness properties of the source have a profound effect on the security of the encryption, with several examples of compromised

1. Introduction

Information security [1] is a foundation of modern infrastructure with quantum optics set to play a prevalent role in the next generation of cryptographic hardware [2]. Randomness is a core resource for cryptography and considerable effort has gone into making systems suitable for supplying high bit rate streams of random bits. The randomness properties of the source have a profound effect on the security of the encryption, with several examples of compromised
security from an attack on the random number generator [3–5]. In this area, quantum optics has provided advantages over previous methods, enabling random number generation with high speeds and enhanced security [6–8].

The gold standard for security in random number generators comes from device independent quantum random number generators (QRNGs) [9], where the output is certified as random regardless of the level of trust in the generator. These generators require an experimental violation of a Bell-type inequality, an extremely difficult task, limiting generation rates to well below practical requirements (<<kbit/s) [10,11]. Other approaches based on the Kochen-Specker theorem to prove value indefiniteness of the measurement, have demonstrated faster but not yet usable generation rates (25kbit/s) [12,13]. Currently, high-speed (Mbit/s-Tbit/s) quantum random number generation relies on trusted or semi-trusted generators, where the independence of the randomness from classical noise is experimentally tested [14–21]. While these systems have no quantum physical guarantee of their randomness, they are usually denoted as QRNGs due to the quantum mechanical origin of the randomness.

Multiplexed quantum random number generation has previously been theoretically proposed as a solution to post-processing bottlenecks in the real-time rate of QRNGs [7,8]. Previous demonstrations of a parallel nature remain focused on increasing single-channel data rates. Gräfe et al. extend single photon path-encoding based QRNGs to the multi-mode case increasing the bitrate for a fixed measured photon flux [22]. Haw et al. sample two separate frequency slices of their homodyne detector bandwidth in a vacuum fluctuation QRNG, enabling them to generate randomness at twice their digitization rate [23]. Both demonstrations remain ultimately rate-limited by generation [22] or detection [23] rates. However, the goal of multiplexing should be to increase the data rate regardless of single channel bandwidth limitations. A multiplexing architecture is more versatile than increasing the rate of a single data stream, allowing the use of more complex extraction techniques and randomness distribution at rates faster than a single channel capacity. For example, a server may possess one parallel QRNG, and send encrypted data to many clients at maximum single channel capacity simultaneously. Similarly, many clients may access random numbers from a server at the same time. In the same way, high bit rate data transmission relies on parallelisation, and as such parallel QRNG is an innate match for encryption of such links.

A second major advantage comes in the randomness extraction technique. Randomness extractors are algorithms which, given a bit string from a weakly random physical source, produce a shorter sequence of truly random bits [24]. Previous works have largely used seeded extractors, which require a uniform random seed to convert the input to random bits. Such extraction is often described as randomness expansion, as it cannot extract true randomness without already having some at the input [6]. Seeded extractors rely on the uniformity of the seed and independence of the output from this seed for security. We can relax both of these requirements with a multi-source extractor.

A single random output is produced from two weakly random inputs in a multi-source extractor. The main advantage of this approach is that random numbers can be generated without any initial random seed. Many examples of multi-source extractors exist that allow for unseeded extraction with low entropy loss, including constructions which are strong extractors in the presence of quantum side information [25].

We experimentally demonstrate the first parallel quantum random generator whose total rate is not limited by generation or detection rates but rather by the number of parallel channels used. Furthermore, we demonstrate the versatility of the de-multiplexed nature of our scheme to implement a strong extractor, whose security does not rely on a pre-prepared seed, using a two-source extractor design. We demonstrate three different randomness extraction techniques starting from a raw random number generation rate of 3.08 Gbit/s, from 27.5 MHz detector bandwidth. Secondly, we implement a cryptographic hash function to extract uniform randomness in accordance with NIST draft standards for random number generation. Finally,
we exploit the multiplexed nature of our system with an unseeded theoretically-strong extractor [26] that combines two independent random sources and show a generation rate of 26 Mbit/s.

2. Random Number Generation Scheme

The schematic of our multiplexed QRNG is shown in Fig. 1. The noise source of each channel of our multiplexed design comes from homodyne measurements of vacuum state [21,27] (see inset in Fig. 2(a)). A laser is sent onto a 50-50 beamsplitter while vacuum enters the other port, subsequently the two outputs of the beamsplitter are detected on two photodiodes and the difference between the two photocurrents is amplified by an amount G. The homodyne current is proportional to a measurement of the quadrature operator of the vacuum state, and its value is independent and unpredictable within a Gaussian distribution with zero mean. This current can equivalently be viewed as arising from the shot noise of the light incident on the photodiodes.

The homodyne detectors used in this demonstration follow the design of Kumar et al. [28] and have an electronic bandwidth of ~100MHz. The quantum signal to classical noise ratio (QCNR) is defined as $QCNR = 10 \log_{10}(\sigma_Q^2/\sigma_E^2)$ where $\sigma_Q^2$ is the quantum noise variance. It can be calculated from the variances of the vacuum state and classical noise measurements $\sigma_M^2$ and $\sigma_E^2$ using $\sigma_M^2 = \sigma_Q^2 + \sigma_E^2$. Fig. 2(a) shows the results for all seven homodyne detectors. We see that for all channels of our design this ratio exceeds 10dB across 30 MHz, with a measured common mode rejection ratio of >27dB across all seven detectors. To confirm that our detectors were measuring vacuum fluctuations, we determine the linearity of the noise as a function of the laser power (see Fig. 2(b)). The independence of the outcomes of each of the channels was verified from cross-correlation measurements shown in Fig. 2(c). The standard deviation of the cross-correlations for ideal uniform data is $1/\sqrt{n} = 3.16 \times 10^{-4}$. The standard deviation of all 21 channel pairing cross-correlations lies between $2.83 \times 10^{-4}$ and $3.51 \times 10^{-4}$.

Fig. 1. Experimental setup for multiplexed quantum random number generator based on quadrature measurements of the vacuum state. A low noise, Koheras Boostik laser at 1550nm is coupled in and out of a lithium niobate waveguide network through butt-coupled fiber arrays. Light from the outputs is sent into seven homodyne detectors. The detector signals are sent to the ADC and FPGA for digitization, processing and randomness extraction.

Integrated optics provides a compact and stable way to implement the set of beamsplitters needed to feed many homodyne detectors. We fabricate a 1:32 multiplexer using annealed proton exchanged waveguides in lithium niobate with a device footprint of 60mm x 5mm [29]. The device has insertion losses of ~7 dB and we choose seven pairs of outputs with balanced power to send to the seven homodyne detectors. Our choice of lithium niobate is designed for a semi-integrated system, where a laser, the waveguide device, a butt coupled linear photodiode array, and all the electronics are on a single circuit board. Lithium niobate offers a reliable, low loss fabrication platform, with simple alignment for butt-coupling.
Several data processing steps are implemented in order to transform the analog signals from the homodyne detectors into a stream of random bits (see Fig. 1). First, the analog output of each detector is digitized into 12 bits per sample using an analog to digital converter (ADC, Texas Instruments ADS5295EVM). In our demonstration no anti-aliasing filter is used and as such frequencies higher than the detection bandwidth contribute to the signal. The digitized results from each outcome are sent in parallel into a field programmable gate array (FPGA, Altera Arria II GX Development Kit) for the remainder of the randomness extraction protocols. If the outputs are to be multiplexed back together rather than used in parallel, multiplexing occurs after the randomness extractor.

Three different extraction methods are demonstrated that convert the unpredictable measurement outcomes of the homodyne detectors into random bit streams. In the first extractor (A), which we call 'raw bit extraction', we take the eight least significant bits (LSBs) from the ADC and discard the remaining 4 bits per sample. This extractor follows the design of the 'environmental immunity' procedure of [30].

The second extractor (B) is based on the second draft of NIST Special Publication 800-90B[31]. The authors list a set of vetted randomness extractors, one of which is the keyed algorithm CMAC (Cipher-based Message Authentication Code)[32] with the AES (Advanced Encryption Standard) [33] block cipher. For an input with k bits of min-entropy i.e., one where the maximum probability of any outcome is bounded by $2^k$, when $\leq k/2$ bits are taken from the 128 bit output of the extractor, full-entropy output bits are produced [31]. The remaining $\lfloor 128 - k/2 \rfloor$ bits are used to refresh the seed. We take eight LSBs from sixteen consecutive digitization samples to form the 128-bit input to each run of the extractor. The AES hash is implemented on the FPGA using the TinyAES core[34].

The third extractor (C) takes advantage of the fact that we have many independent sources, and as such can use a multi-source extractor. Examples of both weak (seed-dependent, non-reusable seed) and strong (seed-independent, reusable seed) extractors have been shown for QRNGs. The security of these extractors relies on the quality of the previously created random seed. Multi-source extractors discard the necessity for a truly random seed. Instead, they take two or more partially random bit-strings from weak randomness sources and produce a truly random output. Given sufficient randomness of the inputs, a strong multi source extractor outputs bits that are uncorrelated with any of the inputs, providing randomness even with full knowledge of all but one of the inputs. We implement a single bit two-source extractor, as
described in [26]. Each extractor takes two 36-bit strings from two different homodyne
detectors, each consisting of three 12-bit samples. Using six of the detectors we create three of
these extractors and multiplex the outputs together.

3. Entropy Source Evaluation

We first evaluate the worst-case conditional min-entropy of the 12-bit output of the ADC for
each channel to find the amount of entropy sourced from the measurement of the vacuum state.
The worst-case conditional min-entropy ($H_{\text{min}}$) provides a lower bound for the maximum
extractable randomness given the discretized measured distribution conditioned on the classical
side information [35]. Using the procedure described by Haw et al. [23] for a discretized
conditional probability distribution with classical noise bounded by $\epsilon_{\text{max}}$ we numerically
evaluate the worst-case conditional min-entropy for a QCNR of 10dB using a representative
sample of $1 \times 10^6$ samples per channel. We find that for all seven channels $H_{\text{min}} \geq 9.201$ bits
per 12-bit sample, meaning these bits are secure against classical side information, up to a
maximum classical noise spread of $\epsilon_{\text{max}} = 5\sigma_c$, for a near optimal digitization range. This value
describes the entropy component immune to classical noise sources; however, it does not
describe the component immune to quantum side information, as the extractors we use are not
secure against such attacks.

If each sample in a test set from a noise source is mutually independent and have the same
probability distribution, that noise source is considered to be independent and identically
distributed (IID). The NIST SP800-90B entropy assessment package [36] uses a range of
statistical tests to attempt to prove that a sample is not IID. If none of the tests fail, the noise
source is assumed IID. The output entropy of the raw bit extraction is tested using the entropy
estimate procedure from NIST SP800-90B, and find the sample passes the IID test with an
entropy of 7.897 bits. The total bit rate of this construction is given by the product of the sample
rate (55MSPS), extracted bits per sample (8), and number of channels (7), and is 3.08 Gbit/s.
The sampling rate is limited by the interface between the ADC and FPGA, and as such, we
sample 27.5 MHz of the homodyne detector bandwidth. Thus, we generate 112 Mbit/s per MHz
of single channel detector bandwidth. We note that previous implementations have sampled
more than an order-of-magnitude more detector bandwidth with superior detectors and
digitization [23], which will enable parallel QRNG from vacuum to reach much faster rates
than in this demonstration.

Table 1. Summary of results for our three constructions.

<table>
<thead>
<tr>
<th></th>
<th>Raw 8Bit</th>
<th>AES</th>
<th>TwoSource</th>
</tr>
</thead>
<tbody>
<tr>
<td>Min-Entropy per 8 bits</td>
<td>7.897</td>
<td>7.902</td>
<td>7.890</td>
</tr>
<tr>
<td>IID Test[31]</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
</tr>
<tr>
<td>Generation Rate</td>
<td>3.08 Gbit/s</td>
<td>1.37 Gbit/s</td>
<td>26Mbit/s</td>
</tr>
<tr>
<td>Randomness Test[37]</td>
<td>Pass</td>
<td>Pass</td>
<td>Pass</td>
</tr>
</tbody>
</table>

Using this entropy estimate of the 8-bit raw data we construct a CMAC keyed extractor (B),
taking 63 out of 128 bits of the output to ensure the number of bits we use is less than half the
input entropy. Entropy tests of the output give a min-entropy of 7.902 bits and the sample passes
the IID test. Finally, we measure the output entropy of our two-source extractor (C) to be 0.986
bits as it is a single bit extractor, and it also passes the IID test. The results for all three extractors
are summarized in Table 1. The NIST statistical test suite [37] is also used to identify any
statistical correlations that may make the data non-random. We run the test suite on each of our
constructions over a minimum sample size of $7 \times 10^8$ bits and find extraction methods A, B, and C pass all tests.

![Correlation between the output of a single two-source extractor and its inputs 1(a) and 2(b). Both positive (squares) and negative (triangles) correlations are plotted, with the y-axis shared between plots.](image)

The two-source extractor we implement is strong given perfectly independent inputs i.e., the output is uncorrelated to either of the inputs. We quantify the effect of experimental imperfections in the input independence by calculating the cross-correlation between each input and the output as a measure of extractor strength, shown in Fig. 3 for $4.3 \times 10^6$ samples. The theoretical correlation of perfectly random data for the sample size is $4.8 \times 10^{-4}$.

4. Conclusion

In summary, we have demonstrated the first parallel/multiplexed quantum random number generator, a configuration ideally suited to a range of platforms, as well as capable of enhancing real time QRNG rates. Parallelisation of random number generation is an effective way to increase the real-time bit rate of QRNG’s, supply of quantum random numbers to distributed or cluster based computation and parallel communication systems.

Furthermore, the parallel architecture allows us to demonstrate a high-speed un-keyed strong extraction to create random numbers without the need for an external provider of uniform random seeds. True randomness sources that do not need a random seed have practical security by relying only on the validity of the partially random sources, and not requiring an external source of true randomness.

With our integrated device, up to sixteen channels can be used simultaneously, given sufficient detectors and electronics. The parallel processing ability of an FPGA makes it ideal for the task of randomness extraction across many channels in parallel. Additionally, multi-channel high speed ADC’s are readily available. The highly specialized nature of the electronic components makes a system on a single circuit board the realistic short-term integration option. To continue the scaling of this system to hundreds of channels full integration of the laser, waveguides, photodiodes, and processing electronics on a single chip will be necessary, and silicon offers a suitable platform for both electronic and optical components [38].

Funding

Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (CE170100012); Griffith University Research Infrastructure Programme.

Acknowledgments
The authors thank Stefan Morley and Xingxing Xing for electronics support and Zachary Vernon for comments on the manuscript. BH is supported by the Australian Government Research Training Program Scholarship. This work was performed in part at the Queensland node of the Australian National Fabrication Facility, a company established under the National Collaborative Research Infrastructure Strategy to provide nano- and microfabrication facilities for Australia's researchers.
5. Integrated generation, manipulation and detection of squeezed light

5.1. Statement of contribution to co-authored published paper

This chapter includes a co-authored paper. The status of the co-authored paper, including all authors, is:

Francesco Lenzini, Jiri Janousek, Oliver Thearle, Ben Haylock, Matteo Villa, Sachin Kasture, Liang Cui, Hoang-Phuong Phan, Dzung Viet Dao, Hidehiro Yonezawa, Ping Koy Lam, Elanor Huntington, and Mirko Lobino, “Integrated photonic platform for quantum information with continuous variables” submitted to Science Advances

A summary of all author contributions is present in the included paper.

My contribution to the paper involved:

- With author 1, 5, 6, and 14 design and fabrication of the integrated device
- With all authors, preparation of the manuscript

(Signed) (Date) 27/07/2018
Benjamin Haylock

(Countersigned) (Date) 27/07/2018
Corresponding author of paper: Mirko Lobino

(Countersigned) (Date) 27/07/2018
Supervisor: Mirko Lobino
5.2. Integrated generation, manipulation and homodyne detection of continuous variable entanglement

This project was one of the main goals during development of fabrication facilities for the Integrated Quantum Technologies group. We considered it a significant achievement if we could generate, manipulate, and perform homodyne interferometry of squeezed states in a single chip. This led to the development of our waveguide, periodic poling, and electrode fabrication technologies, and indeed lithium niobates ability to host all three processes made it the standout choice for this project and led to the other spin off technologies already presented. The presence of two of the world's leading experts on continuous variable quantum information, Professors Ping Koy Lam and Elanor Huntington at the Australian National University meant it was a natural choice to perform the experimental verification of the chip design in Canberra, working with their groups.

The future goal of this project will be to demonstrate violation of a Bell-type inequality on chip. For present the level of squeezing generated is insufficient to achieve that, however further improvements to the fabrication process will bring us closer to that goal. Dr Lenzini and A/Prof Lobino also noted its relevance to time-multiplexed continuous variable cluster state quantum computing, and indeed this circuit can be used as a fundamental building block for its experimental implementation. This work expands upon previous integrated quantum optics demonstration by performing the first demonstration of integrated generation, active manipulation, entanglement, and detection of quantum states on a single chip. Using the advantages of integration, we show the extensibility of our platform to continuous variable quantum information tasks.

5.2.1. Included Paper - Integrated photonic platform for quantum information with continuous variables

The remainder of this page is intentionally left blank.
Integrated photonic platform for quantum information with continuous variables

Francesco Lenzini1,2, Jiri Janousek3,4, Oliver Thearle3,4, Matteo Villa1, Ben Haylock1, Sachin Kasture1, Liang Cui5, Hoang-Phuong Phan6,7, Dzung Viet Dao6,7, Hidehiro Yonezawa8, Ping Koy Lam4, Elanor H. Huntington3, and Mirko Lobino1,6,*

1 Centre for Quantum Computation & Communication Technology and Centre for Quantum Dynamics, Griffith University, Brisbane QLD 4111, Australia
2 Institut of Physics, University of Muenster, 48149 Muenster, Germany
3 Centre for Quantum Computation & Communication Technology and Research School of Engineering, The Australian National University, Canberra ACT 2601, Australia
4 Centre for Quantum Computation & Communication Technology and Department of Quantum Science, Research School of Physics and Engineering, The Australian National University, Canberra ACT 2601, Australia
5 College of Precision Instrument and Opto-electronics Engineering, Tianjin University, Tianjin 300072, China
6 Queensland Micro- and Nanotechnology Centre, Griffith University, Brisbane QLD 4111, Australia
7 School of Engineering, Griffith University, Brisbane QLD 4111, Australia
8 Centre for Quantum Computation & Communication Technology and School of Engineering and Information Technology, The University of New South Wales, Canberra, ACT 2600, Australia
* m.lobino@griffith.edu.au

Integrated quantum photonics provides a scalable platform for the generation, manipulation, and detection of optical quantum states by confining light inside miniaturized waveguide circuits. Here we show the generation, manipulation, and interferometric stage of homodyne detection of non-classical light on a single device, a key step towards a fully integrated approach to quantum information with continuous variables. We use a dynamically reconfigurable lithium niobate waveguide network to generate and characterize squeezed vacuum and two-mode entangled states, key resources for several quantum communication and computing protocols. We measure a squeezing level of $-1.38 \pm 0.04$ dB and demonstrate entanglement by verifying an inseparability criterion $J = 0.77 \pm 0.02 < 1$. Our platform can implement all the processes required for optical quantum technology and its high nonlinearity and fast reconfigurability makes it ideal for the realization of quantum computation with time encoded continuous variable cluster states.

Integrated quantum photonics [1] has emerged as the ideal platform for the implementation of optical quantum computation [2], communication [3], and sensing protocols [4]. By confining light inside miniaturized waveguide circuits, it is possible to generate quantum states of light [5,6], interfere them over waveguide networks [7], and detect them with integrated detectors [8]. Integration of these three key operations establishes the stability and scalability of this technology, enabling a continuous increases in complexity and capabilities of these devices [9,10].

Optical quantum information is more commonly encoded in one of the discrete degrees of freedom (or discrete variables, DV) of single photons such as polarization [11] or path [2]. This approach enables operations with near-unity gate fidelity [12], but is currently limited by the lack of on-demand single photon sources and deterministic two photon quantum gates. The encoding of information on operators that are continuous variables (CV) such as quadrature amplitudes, offers the advantages of deterministic generation of quantum states and operation, at the expense of a higher tendency to imperfect gate fidelities [13]. This approach has been demonstrated in several fields, including secure quantum communication [14], quantum enhanced sensing [15], and quantum information processing [16]. Hybrid approaches combining the benefits of DV and CV systems have also been proposed and experimentally demonstrated [17].

While integrated optics provides great stability and scalability to all types of encoding, in CV schemes it also greatly simplifies the configuration of current experimental setups, replacing phase-locked cavities for generation of squeezed light with single-pass waveguides [18]. It also eliminates the need of mode-cleaning cavities for homodyne detection thanks to the nearly-perfect overlap between optical modes in guiding structures [19,20].

Furthermore, the possibility of achieving broad generation bandwidths in a single-pass squeezer [21], and performing fast-switching operations with electro-optically tunable waveguides [11,22], makes integrated optics an attractive platform for the implementation of frequency [23,24] or time-multiplexed encoding [25,26] and fast feedforward operations needed for CV measurement-based quantum computing [27].
Here we demonstrate a nonlinear and reconfigurable integrated device which generates, actively manipulates, and performs the interferometric stage of homodyne detection on non-classical light fields. The device is formed by two integrated sources of squeezed vacuum and electro-optically tunable phase shifters and beam splitters where squeezed vacua can interfere and be characterized. Complemented with photon-number resolving detectors or non-Gaussian ancilla inputs [13], such architecture can enable non-Gaussian operations for universal quantum information processing or hybridisation with DV systems [17].

Figure 1 shows a schematic of the integrated chip and the experimental setup. The device is made of a network of six waveguides patterned on a Z-cut lithium niobate substrate by reverse proton exchange [28] (see Methods for details on the fabrication process).

Two periodically poled waveguides, phase-matched around 1550 nm, are used to generate two squeezed vacuum states which are interfered on a reconfigurable directional coupler (DC1) for the generation of a two-mode CV entangled state [13]. Both waveguides have a 2 cm interaction length, extrapolated from the 0.5 nm FWHM of the second harmonic generation efficiency as a function of the pump wavelength (Fig. 2a). This interaction length corresponds to a 96 nm FWHM bandwidth for the generated squeezed light.

Two directional couplers (DC2, DC3) designed with a 100% splitting ratio (SR) at 1550 nm separate the generated quantum states from the pump beams, which remain confined in the initial waveguides due to the smaller mode field diameter. Balanced homodyne detection is performed by mixing the generated signals with two local oscillator beams in two tunable directional couplers (DC4, DC5). Electrodes patterned on top of the waveguides are used to scan the phase of the local oscillators, and to tune the SR of the directional couplers [22]. Local oscillator phases $\phi_{LO1}$ and $\phi_{LO2}$ are scanned by $2\pi$ when a ±10 V waveform is applied (see Fig. 2b and c), while the splitting ratios of the reconfigurable couplers can be reduced from their no voltage values down to ~0.5% with an applied voltage in the ±20 V range (see Methods). The SRs of DC4 and DC5 are tuned at around 50% for balanced homodyne detection.

Two mode CV entanglement is generated by interfering orthogonal squeezed vacuum states from the two periodically poled waveguides on DC1 with a SR tuned at 50%. Separable squeezed vacuum states are created when the SR of DC1 is set as close as possible to zero (~0.5%), for implementing the identity operation. Due to imperfections in the waveguide fabrication process the SR of DC2, DC3 was found equal to 80% and 86% respectively, reducing, in this way, the maximum amount of measurable squeezing. In future implementations the performance of the filters could be improved by patterning electrodes with alternating phase mismatch [29], to allow tuning the SR in the full 0-100% range.

The master laser is an amplified cavity diode laser, based on a gain chip [30], and tunable in the 1550 nm wavelength range. The pump beam is obtained by frequency doubling part of the master laser power with a PPKTP crystal in a single-resonant cavity (see Methods), with the remaining power used as local oscillators. All the beams are coupled into the chip with a fiber V-groove array, while the output modes are collected by a 0.5NA lens and sent to a pair of homodyne detectors (HD1, HD2) with 99% quantum efficiencies (see Methods). Electronic filtering is used to select a wide side-band from 4 MHz to 35 MHz, which is measured in the time-domain with a digital oscilloscope. For generation of CV entanglement, the relative phase of the two pump beams

![Diagram](image_url)
is controlled in free-space with a piezo-electric mirror. The second and fifth inputs of the device were unused in this experiment, but in future may be used to implement displacement operations [13,17].

**FIG. 2.** Generation and homodyne detection of squeezed vacuum states. (a) Measured normalized second harmonic generation (SHG) efficiencies $P_{2\omega}/P_\omega^2$ for waveguide 1 (blue points) and waveguide 2 (red points) at $T = 125$ °C and relative theoretical fit (solid lines). Pump and second harmonic powers are corrected for Fresnel losses at the output facet and propagation losses (see Methods). The FWHM of the fit sinc$^2$ are $\approx 0.5$ nm, consistent with a $\approx 2$ cm interaction length. The waveguides have the same normalized conversion efficiency $\approx 370$ %W$^{-1}$ at $\lambda = 1554.45$ nm. (b), Splitting ratio of DC1 (top image), and voltage applied to the local oscillator phase shifters (bottom image) as a function of time. SR measurement is performed by injecting a 1550 nm beam into waveguide 2 and measuring the power at the first output with a photodiode. DC1 electrode is driven with a square wave with 1 kHz frequency and $\pm 16$ V amplitude. Distortion of the square signal is due to the limited bandwidth of the voltage amplifier. (c), Noise trace measured from HD1 for a 154 mW pump power. Noise variance is calculated on time intervals of 4 µs duration and averaged over 40 sequential traces. Sampling rate is 50MSPS. (d), Measured squeezing and anti-squeezing levels as a function of pump power for waveguide 1 (blue squares) and waveguide 2 (red circles). Solid lines are the fits made with the function of Eq. 1. Error on the measured noise levels is ±0.04 dB. Pump powers are measured at the output of the device and corrected for Fresnel losses at the output facet and propagation losses inside the waveguides. Pump wavelength is $\lambda_P = 1554.55/2$ nm for waveguide 1, and $\lambda_P = 1554.35/2$ nm for waveguide 2.

The device was first configured for generation and homodyne detection of squeezed vacuum states. SR of DC1 was set to the minimum value of 0.5%, and the phases of local oscillator beams scanned by approximately $2\pi$ with a ramp function (see Fig. 2b). To prevent accumulation of surface charge due to the application of a DC offset, the three directional couplers were modulated by a square function with zero mean amplitude and a 1 kHz frequency. Post-processing on the acquired signal was used to select a 0.4 ms time window centred around the applied square waves every modulation period. Characterization was carried out by injecting a pump beam into each periodically poled waveguide at a time, and measuring the resulting noise levels on the adjacent homodyne detectors. Due to the high operational temperature ($T = 125$ °C), the coupled pump power inside the waveguides can be increased up to $\approx 160$ mW without any evidence of photorefractive damage.

Figure 2c shows the noise trace from HD1, corresponding to a maximum measured squeezing (anti-squeezing) level $\langle \Delta^2 \hat{X}^+ \rangle = -1.38 \pm 0.04$ dB ($\langle \Delta^2 \hat{X}^- \rangle = 1.98 \pm 0.04$ dB) for a pump power $P = 154$ mW. After correcting for 13% Fresnel losses, which could be eliminated with an anti-reflection coating on the output facet, and inefficiencies of the filter (SR=80%), we estimate that $-2.15\pm0.04$ dB of squeezing is generated in our device. The squeezing and anti-squeezing levels measured for both waveguides as a function of pump power are shown in Fig. 2d. The points are fitted using the function
\( (\Delta^2 \hat{X}^\pm) = \eta e^{\pm 2 \mu \sqrt{P}} + 1, \) 

(1)

where \( \eta \) is the overall detection efficiency. Results of the fit give \( \mu_1 = 0.030 \pm 0.001 \) mW\(^{-1/2} \), \( \mu_2 = 0.027 \pm 0.001 \) mW\(^{-1/2} \), \( \eta_1 = 0.52 \pm 0.02, \) and \( \eta_2 = 0.54 \pm 0.02 \), against estimated \( \eta_1 = 0.55 \), and \( \eta_2 = 0.6 \), for 0.14 dB/cm propagation losses (see Methods). We note that \( \eta_1 \) is found compatible, within the 95% confidence interval, with the estimated value. For waveguide 2, the extra 0.06 inefficiency is likely introduced by imperfections in the waveguides along the path of the generated signals.

FIG. 3. Generation and characterization of CV entanglement. (a) Splitting ratio of DC1 (top image), and voltage applied to phase shifters \( \phi_01 \) (green trace, bottom image) and \( \phi_02 \) (red trace, bottom image) as a function of time. SR measurement is performed by injecting a 1550 nm beam into waveguide 2 and measuring the power at the first output with a photodiode. DC1 electrode is driven with a square wave at 1 kHz frequency and ±5.5 V amplitude. Scanning frequency is 1 kHz for \( \phi_01 \) and 10 kHz for \( \phi_02 \). (b) Noise levels measured from HD1 (blue trace) and HD2 (red trace) when the pump beams are in phase. (c) Noise levels measured from HD1 (blue trace) and HD2 (red trace) when the pump beams are out of phase. (d) Noise levels of summed quadratures \( (\Delta^2 \hat{X}_1 \pm \hat{X}_2) \) (green trace) and subtracted quadratures \( (\Delta^2 \hat{X}_1 - \hat{X}_2) \) (red trace) when the pump beams are out of phase. Noise variance is calculated on time intervals of 2.5 µs duration and averaged over 10 sequential traces. Sampling time is 20 ns. Measurements are performed with two pump beams with \( P = 122 \) mW and \( \lambda_p = 1554.45/2 \) nm.

Next, the device was configured for the generation and characterization of CV entanglement between the two spatial modes after DC1. SR of DC1 was set to 50% and the phases of the two local oscillator beams were scanned by approximately \( \pi \) at 1 kHz for \( \phi_01 \) and 10 kHz for \( \phi_02 \) (see Fig. 3a). The phase of pump 1 was scanned simultaneously by approximately 2\( \pi \) at a much lower speed (50 Hz) using a piezo-electric mirror (see Fig. 1). Entanglement was verified using the inseparability criterion for Gaussian states [31]

\[
I = \sqrt{\min[(\Delta^2 \hat{X}_1^+ \pm \hat{X}_2^+)] \times \min[(\Delta^2 \hat{X}_1^- \pm \hat{X}_2^-)]} < 1,
\]

where we use the product form of Ref. 31, and \( \hat{X}_-^-, \hat{X}_+^+ \) are, respectively, squeezed and anti-squeezed quadratures when the pump beams are in phase.

Figures 3b-d show the results of the measurements for a 122 mW pump power coupled in each waveguide. When the pump beams are in phase (Fig. 3b), the device generates two separable squeezed states with similar squeezing and anti-squeezing levels, \( (\Delta^2 \hat{X}_{1^+}^-) = -1.16 \pm 0.06 \) dB, \( (\Delta^2 \hat{X}_{2^+}^-) = 1.71 \pm 0.06 \) dB for HD1, and \( (\Delta^2 \hat{X}_{1^-}^+) = -1.11 \pm 0.06 \) dB, \( (\Delta^2 \hat{X}_{2^-}^+) = 1.65 \pm 0.06 \) dB for HD2. When the pump beams have a \( \pi \) relative phase (Fig. 3c), as expected
for an entangled state, we observed phase independent and constant noise levels \(\langle \Delta^2 \hat{X}_1 \rangle = 0.53 \pm 0.20 \text{ dB for HD1, and } \langle \Delta^2 \hat{X}_2 \rangle = 0.54 \pm 0.20 \text{ dB for HD2. Conversely, variance of summed and subtracted quadratures (green and red traces in Fig. 3d) show a phase-sensitive behaviour with correlations below the equivalent shot noise level resulting from the combination of the two homodyne currents (see Methods). From the data of Fig. 3d we calculated min\(\langle \Delta^2 (\hat{X}_1^2 \pm \hat{X}_2^2)\rangle\rangle = -1.19 \pm 0.12 \text{ dB, and min}[\Delta^2 (\hat{X}_1^2 \pm \hat{X}_2^2)] = -1.07 \pm 0.12 \text{ dB, corresponding to } I = 0.77 \pm 0.02 < 1 \) which satisfies the inseparability criterion by 11 standard errors.

In conclusion we demonstrated the generation, manipulation, and characterization of nonclassical quantum states of light in a monolithically integrated device. We have shown the reconfigurability of our technology by generating squeezed vacua and CV quadrature entanglement in two separate spatial modes. We calculated that by increasing the peak power to 500 mW with a pulsed pump laser and the interaction length to 4 cm, our fabrication technology could reach ~7 dB of squeezing. Furthermore, the recently developed low loss, high confinement ridge waveguides in lithium niobate [32] can potentially generate more than 10 dB of squeezing with this same material and provide a technology with a footprint similar to the silicon-on-insulator platform. In the future it will be of interest to measure this broadband quantum states with high bandwidth homodyne detectors and demonstrate fast-switching operations in the GHz regime for measurement based quantum computation.

**ACKNOWLEDGEMENTS**

We thank Nicholas Robins for lending us the laser. This work was supported by the Australian Research Council (ARC) Centre of Excellence for Quantum Computation and Communication Technology (CE170100012), and the Griffith University Research Infrastructure Program. BH and MV are supported by the Australian Government Research Training Program Scholarship. This work was performed in part at the Queensland node of the Australian National Fabrication Facility, a company established under the National Collaborative Research Infrastructure Strategy to provide nano- and microfabrication facilities for Australia’s researchers.

**AUTHOR CONTRIBUTIONS**


**REFERENCES**


METHODS

Fabrication of the chip

Waveguides were fabricated with a 1.85 µm proton exchange depth followed by annealing for 8 hours at 328 °C, and reverse proton exchange for 10 hours at the same temperature. Inputs of the periodically poled waveguides were designed with a channel width of 2.5 µm to get early single-mode operation at 775 nm and inject efficiently the pump beam into the fundamental mode of the waveguides. Channel width at the beginning of the poling region was increased to 8 µm with a 7 mm adiabatic taper to work in non-critical condition for quasi-phase matching. After the poling region, the channel widths are decreased to 6 µm with a second adiabatic taper of 1.5 mm length to get single-mode operation at 1550 nm. S-bends were designed with a sinusoidal function and a minimum bend radius of 40 mm. Separation between waveguide centres at the input and the output of the device was set to 127 µm to match the standard pitch of fibre V-groove arrays. To prevent back-reflections into the waveguides, the output facet was polished at an 8° angle. Total length of the chip is 62 mm.
The poling pattern was generated by standard electric-field poling with a period \( \Lambda = 16.12 \mu \text{m} \), and a 50:50 duty cycle. After poling and waveguide fabrication, aluminium electrodes are realized on a 200 nm thick SiO\(_2\) buffer layer in order to prevent optical absorption from the metal. Aluminium thickness was 250 nm, while electrodes were patterned using electron-beam lithography and wet etching.

Directional couplers were designed with separation between waveguide centres of 11.3 \( \mu \text{m} \) for DC1, DC4, and DC5, and 10.6 \( \mu \text{m} \) for DC2, and DC3. The lengths of the directional couplers are 6.1 mm for DC1, and 3.5 mm for DC2, DC3, DC4, and DC5. 12 mm long electrodes act as phase shifters on the local oscillator arms. At a zero applied voltage the SRs of the reconfigurable couplers are 72% for DC1, 85% for DC4, and 75% for DC5. Isolation of the pump beams by DC2 and DC3 on the adjacent homodyne detectors channels was found equal to 20 dB.

To prevent photorefractive damage, the chip was bonded with a UV curing glue to a custom-made aluminium oven and heated at 125 °C. Two printed circuit boards with SMA connectors were mounted on the sides of the oven and wire-bonded to the electrodes to control the voltage applied to phase shifters and directional couplers.

### Propagation losses

Transmission of the waveguides at the signal wavelength was tested on the second and fifth waveguides, and at the pump wavelength on the two central inputs. Transmission of the device corrected for Fresnel losses was found equal to 61% at 1550 nm, and to 40% at 775 nm. From numerical calculation of the mode overlap between waveguides and single-mode fibres\(^2\), we estimated 0.14 dB/cm propagation losses at the signal wavelength, and 0.55 dB/cm propagation losses at the pump wavelength. Propagation losses at the signal wavelength were not directly measurable from the central inputs, since 1550 nm beams are only weakly guided in the first tapered section of the periodically poled waveguides.

### Detection efficiencies

Estimation of the detection efficiencies \( \eta_1, \eta_3 \) from Eq. 1 take into account 0.14 dB/cm propagation losses calculated from the centre of the periodically poled waveguides, a 0.5% loss introduced by the first directional coupler, 20% (for waveguide 1) and 14% (for waveguide 2) losses introduced by the pump filters DC2 and DC3, 13% Fresnel losses at the output facet, a 99% QE, and a 17 dB shot-noise clearance measured for a 4 mW local oscillator power.

### Shot-noise levels

To evaluate the shot-noise levels we used a motorized optical chopper blocking periodically the power of the pump beams. For each data acquisition, the shot-noise variance was calculated on five time windows with 0.4 ms duration. Standard error in the evaluation of the shot-noise levels was estimated equal to \( \pm 0.025 \text{ dB} \) and added to all the uncertainties reported in the paper.

### Driving voltage

The electrodes on the chip were driven by three dual channel arbitrary waveform generators. The generators were operated in burst mode with a common trigger generated by a photodiode at the output of the optical chopper. Phase shifters, DC5, and DC1 (for generation of CV entanglement), required voltages in the \( \pm 10 \text{ V} \) range and were driven directly by the waveform generators. DC4, and DC1 (for generation and homodyne detection of squeezed vacuum), required voltages of \( \pm 18 \text{ V} \) and \( \pm 16 \text{ V} \) respectively, generated with two voltage amplifiers. Low-pass filters from DC to 1.9 MHz were used to suppress unwanted amplitude noise introduced by the driving voltage in the measured side-bands.

### Squeezing and anti-squeezing levels

Squeezing and anti-squeezing levels were evaluated by fitting each noise trace with the function

\[
\langle \Delta^2 \hat{X} \rangle = \langle \Delta^2 \hat{X}^+ \rangle \cos^2(at + \phi) + \langle \Delta^2 \hat{X}^- \rangle \sin^2(at + \phi),
\]

where \( t \) is the acquisition time and \( a, \phi \) are fitting parameters. Uncertainties reported in the paper are the standard errors in the evaluation of the coefficients calculated by the least-square fitting procedure.

### Inseparability criterion

Variance of summed and subtracted quadratures were calculated from the photocurrents \( i_1, i_2 \) measured from the two homodyne detectors as\(^\text{17}\)

\[
\langle \Delta^2 (\hat{X}_1 \pm \hat{X}_2) \rangle = \langle \Delta^2 \left( \frac{i_1}{\sqrt{2 \langle \Delta^2 \hat{X}_{SN1} \rangle}} \pm \frac{i_2}{\sqrt{2 \langle \Delta^2 \hat{X}_{SN2} \rangle}} \right) \rangle,
\]

61
where \( \langle \Delta^2 \hat{X}_{SN1} \rangle \), \( \langle \Delta^2 \hat{X}_{SN2} \rangle \) are the shot-noise levels of the two homodyne detectors. Noise variances \( \langle \Delta^2 (\hat{X}_1^+ \pm \hat{X}_2^+) \rangle \), and \( \langle \Delta^2 (\hat{X}_1^- \pm \hat{X}_2^-) \rangle \), were calculated by averaging 4 points centered around the squeezed and anti-squeezed quadrature positions \( X_1^+, X_2^+ \), and \( X_1^-, X_2^- \). Standard error in the evaluation of the noise levels was estimated as

\[
SE = \frac{\sigma_{X_{1,2}}}{\sqrt{4}}
\]

where \( \sigma_{X_{1,2}} \) is the standard deviation of the noise traces measured on each homodyne detector. Due to the finite scanning speed of the second local oscillator phase shifter, the quadratures \( X_1^-, X_1^+ \), used for the calculation of the inseparability criterion have an offset of -0.09 rad and -0.10 rad respectively from the squeezed and anti-squeezed quadrature positions determined when the pump beams are in phase. We point out that the two quadratures are orthogonal within an offset which is smaller than the error in the quadrature positions (±0.02 rad) determined by fitting the data of Fig. 2b. Thus the measured data still satisfies the inseparability criterion, which is generally valid for any set of orthogonal quadratures.

**Homodyne detectors**

The homodyne detectors used in this experiment use two matched photodetectors with custom ordered photodiodes from Laser Components with efficiencies of >99% and dark currents of >20pA. Each photodetector is in a dual amplifier configuration. The first stage uses a DC coupled transimpedance amplifier to amplify the photocurrent using the op amp AD829 with a transimpedance gain of 3k. The signal is then split in two using a resistor network for AC and DC coupled channels. The sidebands containing the measurements are present in the AC signal and the DC signal is used to monitor the detector. The AC path is filtered with a passive high pass filter with a corner frequency of 100 kHz and then amplified with a gain of 20 using another AD829. The DC coupled signal is amplified and used for monitoring. The noise floor of the AC coupled signals from each detector in a homodyne detector is matched using the compensation capacitor on the transimpedance amplifier. The AC signals are matched in phase using cable lengths and then subtracted to get the homodyne signal. The 3dB bandwidth of the homodyne detectors was measured to be 21 MHz and with a local oscillator power of 4 mW, they achieved a dark noise clearance of 17 dB below shot noise.

**SHG cavity**

The SHG cavity is a free-space bow-tie configuration utilising a PPKTP nonlinear crystal. The cavity consists of two high-reflectivity (HR) concave mirrors at 1550 nm with ROC = 50 mm and two plane mirrors. The first plane mirror, input coupler (IC), is a partially reflecting mirror at 1550 nm; the second is a HR steering mirror attached to a piezo actuator. The cavity is locked on resonance utilising PDH technique. All mirrors are anti-reflection (AR) coated at the SHG wavelength. The cavity forms a beam waist of radius of approximately 27 μm between the two concave mirrors, where a 15 mm long PPKTP crystal is aligned. This configuration maximizes the non-linear conversion as detailed by the Boyd-Kleinman theory. The PPKTP crystal is housed in an oven and temperature stabilised around the optimum phase-matching temperature of 40°C using a Peltier element. Both faces of the crystal are wedged and AR coated at both wavelengths to minimise an intra-cavity parasitic interference. 1 W of fundamental optical power is injected through IC into the cavity and converted into the SHG wavelength with 80% efficiency. The SHG field exits the system through one of the concave mirrors and is subsequently coupled into an optical fibre.


6. Conclusion

Presented here are three experiments, each aiming to use the advantages of multiplexed integrated photonics to improve the extensibility of quantum systems. The variety of photonic circuits used were all fabricated at Griffith University in the Integrated Quantum Technologies group. The key results include the creation of a four-photon source from a single quantum dot, an extensible scheme for quantum random number generation without an external seed, and demonstration of the first single chip with integrated quantum light sources, reconfigurable entanglement generation, and detection. Extensions to each of these works have been listed in each chapter. Here suggestions for extension of the presented technology not previously listed are presented.

Chapter 2 described the implementation of an integrated optical switch, for demultiplexing the output of a single micro-pillar quantum dot into many single photon sources. With expected improvements of quantum dot brightness towards 85% in the near future, pumping of the dot and operation of a 20-channel single photon switch at 1GHz can move towards the source parameters needed to perform a large boson sampling experiment.

To achieve a useful 20-fold coincidence rate of 1Hz using 85% efficient detectors, and an ultra-low loss boson sampling circuit with loss of 90% the probability of the switch routing the photon to the correct channel must be >58%. At telecom wavelengths we have fabricated devices with overall transmissions greater than 70%, and switches with extinction ratios of >17dB, meeting these requirements. While recent work has pushed the system size for observing a genuine quantum advantage using boson sampling from the previously assumed 20 photons in 400 modes to 50 photons in 2500 modes\(^{62}\), a 20 photon source still represents a significant technological achievement. To demonstrate a genuine quantum advantage would constitute important experimental work towards the testing of the extended Church-Turing thesis; one of the most important results in computer science.

An alternative approach using the same technology would include the integration of spontaneous parametric down conversion sources, single photon detectors and quantum memories into an optical demultiplexing device as described in 2.2.1 would
enable creation of a fully integrated near deterministic single photon source in lithium niobate. The creation and networking of 20 such sources for a boson sampling experiment is plausible, even if the size of such technology means it would not be extensible to larger demonstrations without moving to LN ridge waveguides. Quantum memories have been demonstrated in doped lithium niobate, however their efficiencies are low\textsuperscript{210}, as similarly are single photon detection efficiencies on lithium niobate\textsuperscript{167}, meaning implementation of such a device is reliant on advances in these two fields.

In Chapter 3 we presented a high speed, multi-channel electronic control box suitable for driving the optical switch presented in Chapter 2. The current design is suitable for driving a ten-channel switch with pulses as short as 2ns. The advent of electrically driven and electrically tuneable quantum light sources\textsuperscript{211}, and the need for fast measurement dependent reconfiguration of photonic circuits for quantum computation means that continuously more complex electronic control systems will be needed for integrated quantum photonics.

Field programmable gate arrays (FPGA’s) offer a solution with much faster processing times than micro-controllers. Their ability to perform high-speed parallel calculations and flexibility in operation provide a control solution on the scale needed for 20-50 photon systems and perhaps even larger before dedicated circuits will be necessary. Alternatively for the continuous variable quantum computation scheme presented by Menicucci\textsuperscript{73}, a single FPGA can control the whole system. An FPGA, with appropriate digital to analogue converters and amplifiers, can control electro-optic modulators for controlling pump and quantum state inputs, actively reconfigure phases and optical switches, and process measurement readouts to feedback to control the photonic circuit.

The quantum random number generation scheme presented in Chapter 4 showed the potential for integrated photonics to increase real-time random number generation rates. The next stage of this project is to improve detection and processing electronics to similar levels per channel to those already demonstrated i.e. 3.5GSPS\textsuperscript{212}. This will allow, even with the same waveguide device, random number generation rates of \approx 25GSPS, and with extension to many more channels, random number generation rates capable of supplying large encrypted networks. While
proton exchange waveguides in lithium niobate have offered a low loss platform for this experiment, integrated platforms with smaller device size, such as silicon, silica, or, LN ridge waveguides, will be necessary to extend this scheme past 128 channels.

In Chapter 5 we have demonstrated simultaneous use of two of the most advantageous properties of lithium niobate, that of its high optical nonlinearity, and large electro-optic effect. It was the first demonstration of quantum light generation, manipulation, entanglement, and interferometric part of homodyne detection all on a single chip.

The first extension of this work is to improve the performance of the device to generate at least 3dB of measured squeezing, allowing for a demonstration of a bell-type inequality violation. The next stage of experimentation after improving performance relates to continuous variable quantum computation and is described in 5.2.1.

This same chip design would also be suitable as a dynamically reconfigurable source of arbitrary Gaussian states. Injecting a displacement beam into one of the local oscillator inputs, setting the splitting ratio of the other directional coupler to zero, and performing homodyne detection off chip would enable creation of arbitrary Gaussian states, within the limitations of the generated squeezing, using a similar scheme to that proposed by Brodutch et al.\textsuperscript{213}.

Another use of the same chip would involve replacing one of the local oscillator inputs with a quantum state, and performing feedforward and dual-homodyne measurement off-chip for an integrated deterministic quantum teleportation device\textsuperscript{214,215}. It is conceivable that with additional components, delay lines, and high-speed feedforward this entire protocol could be integrated into a lithium niobate chip. A pair of these chips could be used for discrete variable entanglement swapping via the scheme of Takeda et al.\textsuperscript{216}. This scheme deterministically swaps entanglement, but only when an entangled discrete variable state is generated. Such schemes have been shown in free space and integration would allow for a more compact and stable implementation, and, with a high performance implementation, be suitable for quantum repeater nodes. Each repeater node would operate using continuous variable measurements, while each link would operate with discrete variables.
In summary, we have demonstrated the advantages to be gained by using multiplexing in integrated photonics for experimental quantum information science, and in particular, the advantages lithium niobate holds over other materials for some applications.
Appendices

Appendix A - List of Co-Authored Papers published during PhD not included elsewhere


Zhengfen Wan, Shujun Wang, Benjamin Haylock, Mirko Lobino, Ivan S Cole, David Thiel, Qin Li “Tuning the subprocesses in laser reduction of graphene oxide by adjusting the power and scanning speed of laser,” submitted to Carbon in January 2018
Bibliography


171. Lenzini, F. Integrated Quantum Photonics with Annealed and Reverse Proton Exchanged Lithium Niobate waveguides. (Griffith University, 2017).


203. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number


