Multiplexed Quantum Random Number Generation

Ben Haylock[1,*], Daniel Peace[1,*], Francesco Lenzini[1], Christian Weedbrook[2], Mirko Lobino[1, 3, #]

[1]Centre for Quantum Dynamics, Griffith University, 170 Kessels Rd, Nathan, Queensland, Australia

[2]Xanadu, 372 Richmond St W. Toronto, Ontario, M5V 2L7, Canada

[3]Queensland 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.

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 proposed as a solution to post-processing bottlenecks in the real-time rate of QRNGs[7,8]. However, a multiplexing architecture is more versatile than increasing the rate of a single data stream in terms of integration with networks with complex topology and allows the use of more complex extraction techniques. For example, a server may possess one parallel QRNG, and send encrypted data to many clients 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[22]. Previous works have largely used weak seeded extractors, which require a non-reusable 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]. The security of seeded extractors relies on the uniformity of the seed and independence of the output from this seed. 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[23].

Here we use waveguide-based optical splitters to generate random numbers from seven independent homodyne detectors in parallel providing a scalable way to increase random number generation rate with a limited detector bandwidth. We also take advantage of the multiplexed nature of our generation to implement a strong extractor, using a two-source extractor design, generating random numbers without a separately prepared random seed. 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 strong extractor[24] 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[21,25] (see inset in Fig. 2a). 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. The quantum signal to classical noise ratio (QCNR) describes how much electronic noise is added to the output by the measurement apparatus and is shown in Fig. 2a for the 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 further confirm that our detectors were measuring vacuum fluctuations, we determine the linearity of the noise as a function of the laser power (see Fig. 2b) while independence between channels was verified from cross-correlation measurements shown in Fig. 2c.

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[26]. 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.

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 digitised into 12 bits per sample using an analog to digital converter (ADC, Texas Instruments ADS5295EVM).

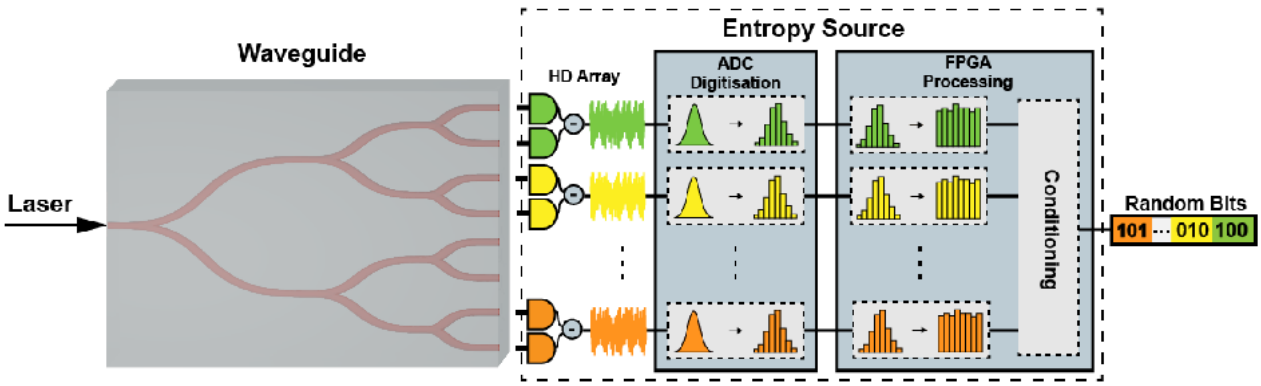

Figure 1: Experimental setup for multiplexed quantum random number generator based on quadrature measurements of the vacuum state. A low noise, Koheras Boostik laser at 1550nm is coupled in and out of a lithium niobate waveguide network through butt-coupled fiber arrays. Light from the outputs is sent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

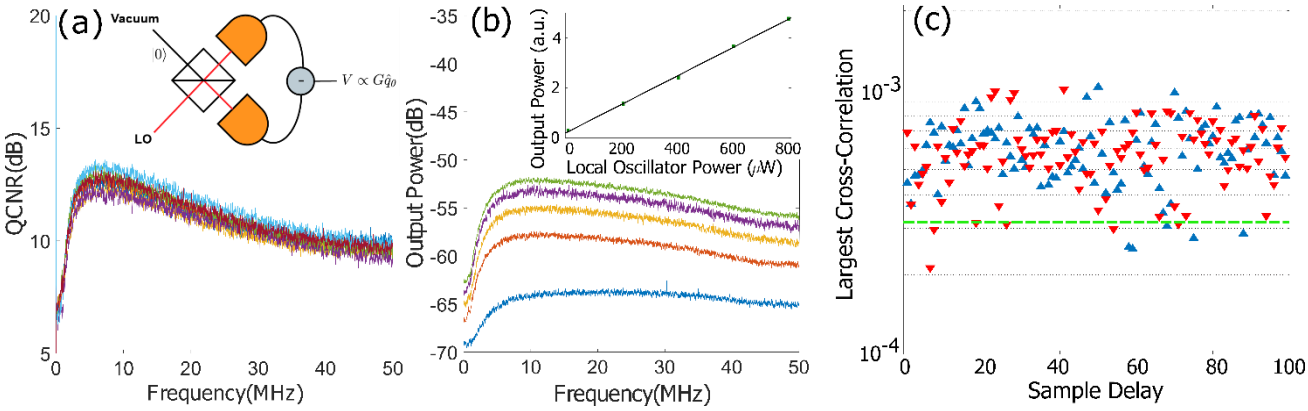

Figure 2: (a) Quantum to classical noise ratio (QCNR) of all seven homodyne detectors used, with inset showing a schematic description of a homodyne detector. (b) Linearity of homodyne detector response with increasing local oscillator power, shown using a representative (channel 4). Blue - 0μW, orange -200μW, yellow - 400μW, purple - 600μW, green - 800μW. The inset shows a plot of the linear response at 5MHz. (c) The largest positive (blue) and negative (red) correlations between any pairwise combinations of eight-bit encoded homodyne measurements from the seven channels. The green line represents the ideal value for the size of the data set (10 million samples).

The digitised 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 Symul et al.[27].

The second extractor (B) is based on the second draft of NIST Special Publication 800-90B[28]. The authors list a set of vetted randomness extractors, one of which is the keyed algorithm CMAC (Cipher-based Message Authentication Code)[29] with the AES (Advanced Encryption Standard)[30] 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[28]. The remaining $\lfloor 128 - k/2 \rfloor$ bits are used to refresh the seed. We take eight LSBs from sixteen consecutive digitisation 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[31].

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. 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, if each input has sufficient randomness. We implement a single bit two-source strong extractor, as described in Ref. 24. 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 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. Conditional min-entropy provides a lower bound for the maximum extractable randomness given the measured distribution X conditioned on the side information K[32,33],

$$H_{min}(X|K) = -\log_2\left[\max_{k_j \in \mathrm{supp}(P_k)} \max_{x_i \in X} P_{X|K}\left(x_i \middle| k_j\right)\right].$$

In our case, the measured distribution is described by a measured variance σ_M^2 conditioned on a measured classical noise variance σ_E^2 . We use conditional min-entropy to describe the input of our extractors and to ensure our entropy description is secure in the presence of classical side information. Using a representative sample of 1×10^6 bits per channel, we find the worst-case min-entropy among all seven channels is 9.201 bits per 12-bit sample conditioned on σ_E^2 up to a maximum spread of $5\sigma_E$.

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[34] 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 detector bandwidth. We note that previous implementations have sampled more than an order-of-magnitude more detector bandwidth with superior detectors and digitisation[33], which will enable parallel QRNG from vacuum to reach much faster rates than in this demonstration.

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 summarised in Table 1.

Table 1: Summary of results for our three constructions.

	Raw 8 Bit	AES	Two Source
Min-Entropy per 8 bits	7.897	7.902	7.890
IID Test[28]	Pass	Pass	Pass
Generation Rate	3.08 Gbit/s	1.37 Gbit/s	26Mbit/s
Randomness Test[35]	Pass	Pass	Pass

The NIST statistical test suite[35] 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 7×10^8 bits and find extraction methods A, B, and C pass all tests.

The two-source extractor we implement has the property that it is a strong extractor i.e., the output is uncorrelated to either of the inputs. We quantify this by calculating the cross-correlation between each input and the output, shown in Fig. 3 for 4.3×10^6 samples. The correlation at all of the first 100 time steps is less than 2×10^{-3} which compares well to the theoretical value for the sample size of 4.8×10^{-4}.

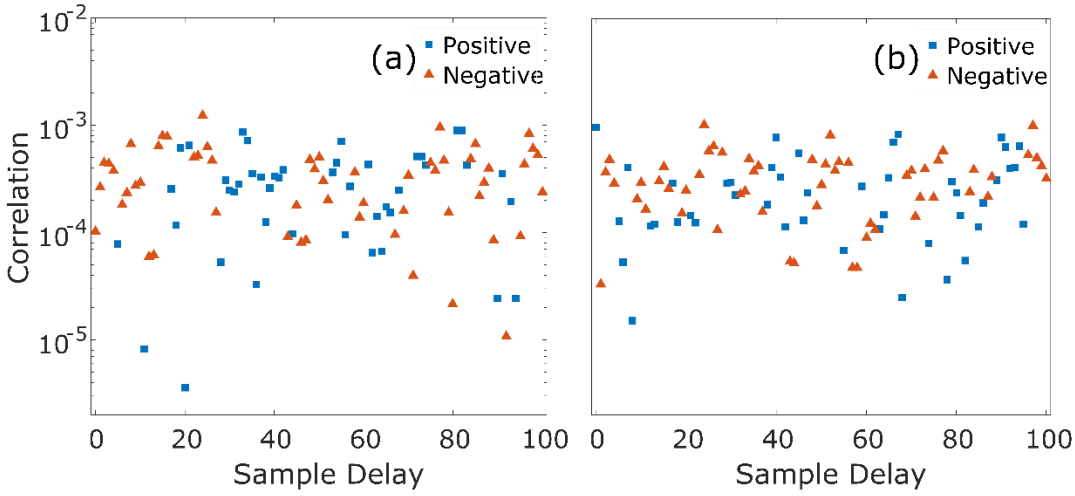

Figure 3: Correlation between the output of a single two-source extractor and its inputs 1(a) and 2(b). Both positive (squares) and negative (triangles) correlations are plotted, with the y-axis shared between plots.

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. To continue the scaling of this system to hundreds of channels, both Indium Phosphide and Silicon offer platforms that could integrate the laser, waveguide network, and homodyne detectors into one chip[36].

References

1. Ware, W. H. Security and Privacy in Computer Systems. in *Proceedings of the Spring Joint Computer Conference* 279--282 (1967).
2. Zhang, P. *et al.* Reference-frame-independent quantum-key-distribution server with a telecom tether for an on-chip client. *Phys. Rev. Lett.* **112,** 1–5 (2014).
3. Debian. Debian -- Security Information -- DSA-1571-1 openssl. (2017). at <https://www.debian.org/security/2008/dsa-1571>
4. Dorrendorf, L., Gutterman, Z. & Pinkas, B. Cryptanalysis of the random number generator of the Windows operating system. *ACM Trans. Inf. Syst. Secur.* **13,** 1–32 (2009).
5. Nohl, K., Evans, D., Starbug & Plotz, H. Reverse-Engineering a Cryptographic RFID Tag. in *17th USENIX Security Symposium* 185–193 (2008).
6. Herrero-Collantes, M. & Garcia-Escartin, J. C. Quantum random number generators. *Rev. Mod. Phys.* **89,** 1–48 (2017).
7. Ma, X., Yuan, X., Cao, Z., Qi, B. & Zhang, Z. Quantum random number generation. *npj Quantum Inf.* **221,** 1–30 (2016).
8. Hart, J. D. *et al.* Recommendations and illustrations for the evaluation of photonic random number generators. *APL Photonics* **2,** 1–22 (2017).
9. Nie, Y. Q. *et al.* Experimental measurement-device-independent quantum random-number generation. *Phys. Rev. A* **94,** 1–5 (2016).
10. Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464,** 1021–1024 (2010).

11. Bierhorst, P. *et al.* Experimentally Generated Random Numbers Certified by the Impossibility of Superluminal Signaling. *arXiv* 1702.05178 (2017). at <https://arxiv.org/pdf/1702.05178.pdf>
12. Kulikov, A., Jerger, M., Potočnik, A., Wallraff, A. & Fedorov, A. Realization of a quantum random generator certified with the Kochen-Specker theorem. *Phys. Rev. Lett.* **119,** 240501 (2017).
13. Abbott, A. A., Calude, C. S., Conder, J. & Svozil, K. Strong Kochen-Specker theorem and incomputability of quantum randomness. *Phys. Rev. A* **86,** (2012).
14. Mitchell, M. W., Abellan, C. & Amaya, W. Strong experimental guarantees in ultrafast quantum random number generation. *Phys. Rev. A* **91,** (2015).
15. Lunghi, T. *et al.* Self-testing quantum random number generator. *Phys. Rev. Lett.* **114,** (2015).
16. Wayne, M. A., Jeffrey, E. R., Akselrod, G. M. & Kwiat, P. G. Photon arrival time quantum random number generation. *J. Mod. Opt.* **56,** 516–522 (2009).
17. Xu, F. *et al.* Ultrafast quantum random number generation based on quantum phase fluctuations. *Opt. Express* **20,** 12366–12377 (2012).
18. Li, L. *et al.* Random Bit Generator Using Delayed Self-Difference of Filtered Amplified Spontaneous Emission. *IEEE Photonics J.* **6,** (2014).
19. Virte, M., Mercier, E., Thienpont, H., Panajotov, K. & Sciamanna, M. Physical random bit generation from chaotic solitary laser diode. *Opt. Express* **22,** 17271 (2014).
20. Marangon, D. G., Vallone, G. & Villoresi, P. Source-Device-Independent Ultrafast Quantum Random Number Generation. *Phys. Rev. Lett.* **118,** (2017).
21. Gabriel, C. *et al.* A generator for unique quantum random numbers based on vacuum states. *Nat. Photonics* **4,** 711–715 (2010).
22. Shaltiel, R. An introduction to randomness extractors. in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* **6756 LNCS,** 21–41 (2011).
23. Kasher, R. & Kempe, J. in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques. Lecture Notes in Computer Science vol 6302* (eds. Serna, M., Shaltiel, R., Jansen, K. & Rolim, J.) 656–669 (Springer, Berlin, Heidelberg, 2010).
24. Bouda, J., Pivoluska, M. & Plesch, M. Improving the Hadamard extractor. *Theor. Comput. Sci.* **459,** 69–76 (2012).
25. Shen, Y., Tian, L. & Zou, H. Practical quantum random number generator based on measuring

the shot noise of vacuum states. *Phys. Rev. A* **81,** (2010).

26. Lenzini, F., Kasture, S., Haylock, B. & Lobino, M. Anisotropic model for the fabrication of annealed and reverse proton exchanged waveguides in congruent lithium niobate. *Opt. Express* **23,** 1748 (2015).
27. Symul, T., Assad, S. M. & Lam, P. K. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Appl. Phys. Lett.* **98,** (2011).
28. Sönmez Turan, M. *et al.* Recommendation for the Entropy Sources Used for Random Bit Generation (Second DRAFT) NIST Special Publication 800-90B. (2016).
29. Dworkin, M. Recommendation for Block Cipher Mode of Operation: The CMAC Mode for Authentication. NIST Special Publication 800-38B. (2005).
30. National Institute of Standards and Technology. Specification for the Advanced Encryption Standard (AES) FIPS 197. (2001).
31. Hsing, H. AES :: Overview :: OpenCores. (2015). at <https://opencores.org/project,tiny_aes>
32. Renner, R. Security of Quantum Key Distribution. *Int. J. Quantum Inf.* **6,** 1–127 (2008).
33. Haw, J. Y. *et al.* Maximization of Extractable Randomness in a Quantum Random-Number Generator. *Phys. Rev. Appl.* **3,** (2015).
34. McKay, K. & Kelsey, J. GitHub - usnistgov/SP800-90B_EntropyAssessment. at <https://github.com/usnistgov/SP800-90B_EntropyAssessment>
35. Rukhin, A. *et al.* A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Rev. 1a.
36. Silverstone, J. W., Bonneau, D., O'Brien, J. L. & Thompson, M. G. Silicon Quantum Photonics. *IEEE J. Sel. Top. Quantum Electron.* **22,** 390–402 (2016).

Acknowledgements

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 supported by the Australian Research Council (ARC) Centre of Excellence for Quantum Computation and Communication Technology (CE170100012), and the Griffith University Research Infrastructure Program. 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

DP and BH built the homodyne detectors and electronics, and performed the experiment. BH and FL fabricated the waveguide network. CW and ML devised the experiment. ML supervised the experiment. All authors contributed to writing.

Competing Financial Interests

The authors declare no competing financial interests.