Multiplexed Quantum Random Number Generation

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

[1]Centre for Quantum Dynamics, Griffith University, Brisbane, 4111, Australia

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

[3]Queensland Micro- and Nanotechnology Centre, Griffith University, Brisbane, 4111, Australia

May 8, 2019

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 real-time 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]. Recent advances[14] have built upon the notion of Bell inequality violations using device independent quantum random number generators. Remarkably, these allow the closure of any security loopholes related to the how the device is made, i.e., independent of the device implementations. 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 [15–22]. 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. This trade-off between speed and security is mostly caused by the experimental complexity of fully secure implementations.

Entropy sources sufficient for randomness generation rates up to 1.2Tb/s have been demonstrated[23], However, these systems are not capable of real time random number generation at full speed due to processing bandwidth limitations, instead performing off-line processing on captured data to generate randomness. Thus these schemes are not suited for providing high-speed random numbers for cryptography. Regardless of generation procedure, implementations of randomness extraction are limited by electronic logic speeds or detection bandwidths. Therefore, for high speed real time random number generation, the most feasible solution is to create many parallel sources with lower entropy rates.

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[24]. Haw et al.

Ben Haylock: This author contributed equally to this work
Daniel Peace: This author contributed equally to this work
Mirko Lobino: m.lobino@griffith.edu.au

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[25]. Both demonstrations remain ultimately rate-limited by generation[24] or detection[25] rates. The goal of multiplexing should be to increase the data rate regardless of single channel bandwidth limitations as shown by IDQuantique by multiplexing together four separate devices on a single interface[26].

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. Randomness extractors are algorithms which, given a bit string from a weakly random physical source, produce a shorter sequence of truly random bits[27]. 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[28].

We experimentally demonstrate a high-speed parallel quantum random generator whose total rate is not limited by generation or detection rates but rather by the number of parallel channels used. While Gbps real-time generation rates have been previously been demonstrated[29–31], our scheme provides a simple method scheme to overcome electronic and processing bandwidth limitations.

2 Random Number Generation Scheme

A schematic of the multiplexed QRNG scheme is shown in Figure 1. The noise source of each channel of our multiplexed design comes from homodyne measurements of vacuum state [15, 32] (see inset in Figure 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. 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.

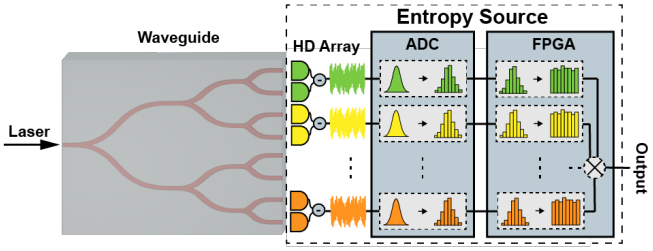

Figure 1: Scheme for multiplexed quantum random number generator based on quadrature measurements of the vacuum state. A low noise, Koheras Boostik laser at 1550nm is coupled in and out of a lithium niobate waveguide network through butt-coupled fiber arrays. Light from the outputs is sent into seven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

The homodyne detectors (HDs) used in this demonstration follow the design of Kumar et al.[33] and have an electronic bandwidth of 100MHz. The quantum efficiencies of the photodiodes used (PD20, oemarket) are >67% (70% typical). The quantum signal to classical noise ratio (QCNR) is defined as QCNR$= 10\log_{10}(\sigma_Q^2/\sigma_E^2)$ where σ_Q^2 is the quantum noise variance, and σ_E^2 is the classical noise variance. Using the equation $\sigma_Q^2 = \sigma_M^2 - \sigma_E^2$, QCNR can be calculated from experimental measurement of the variance of the output of the homodyne detector with the local oscillator off (σ_E^2), and with the local oscillator on (σ_M^2). Figure 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 Figure 2(b)). As the QCNR is the ratio between this response and the value at zero power (blue trace), it also scales linearly with input power. The independence of the outcomes of each of the channels was verified from cross-correlation measurements shown in Figure 2(c). The cross-correlation for ideal uniform data is $1/\sqrt{n} = 3.16 \times 10^{-4}$. All 21 channel pairing cross-correlations lie between 2.83×10^{-4} and 3.51×10^{-4}.

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[34]. The device has insertion losses of ≈7 dB (≈22dB total loss per channel) and we choose balanced outputs to send to the seven homodyne detectors. Total input power to the array is approximately 160mW (≈1mW per channel at output), which will ultimately limit the maximum number of channels. This limitation

may be overcome by using several multiplexed lasers as the input. Our choice of lithium niobate is designed for a semi-integrated system, where a compact butterfly diode laser, the waveguide device, a butt coupled linear photodiode array, and all the electronics could be housed on a single circuit board.

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. Multiplexing is done by interleaving channel by channel and the output of the extractors is written to the on-chip memory of the FPGA and may be transferred to a computer via a USB cable for randomness testing. Randomness verification tests are performed off-line by transferring experimental data to a PC. In any application the memory connected to the FPGA is equally suited to storing and sending the randomness as the memory of a PC.

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 [35]. This extractor is designed to minimise the influence of the classical noise on the output signal. Demonstration of the security of this protocol is through the high entropy of the experimental output, rather than from any theoretical proof.

The second extractor (B) is based on the second draft of NIST Special Publication 800-90B[36]. The authors list a set of vetted randomness extractors, one of which is the keyed algorithm CMAC (Cipher-based Message Authentication Code)[37] with the AES (Advanced Encryption Standard)[38] 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 [36]. 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[39].

The third extractor(C) takes advantage of the fact

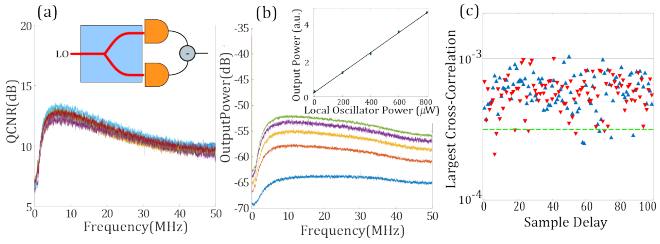

Figure 2: (a) Quantum to classical noise ratio (QCNR) of all seven homodyne detectors used, with inset showing a schematic description of a homodyne detector, orange hemispheres represent photodiodes. Power used is 1mW and all powers are measured at the output of the waveguide device. (b) Linearity of homodyne detector response with increasing local oscillator power, shown using a representative (channel 4). Blue - 0μW, orange -200μW, yellow - 400μW, purple - 600μW, green - 800μW. Inset, 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).

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 [40], which produces a uniform output providing at least one of the inputs has more min-entropy than the output number of bits. Each extractor takes two 36-bit strings from two different homodyne detectors, each consisting of three 12-bit samples. As such we need an even number of input channels for this extractor, and 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. Using the procedure described by Haw et al. [25] for the worst-case conditional min-entropy (H_{min}) we can find a lower bound for the maximum extractable randomness given the discretized measured distribution M_{dis}, conditioned on the classi-

Table 1: Summary of results for our three constructions. The bitrate can be found by multiplication of sampling rate, number of extractors, and extracted bits per sample.The min-entropy per 8 bits for extractor C can be obtained from the reported min-entropy per bit = 0.986 multiplied by eight.

	Raw 8 Bit	AES	Two Source
Extractor Channels	7	7	3
Sampling Rate (MSPS)	55	50	52
Bits per Sample	8	$8 \times 63/128$	$12 \times 1/72$
Generation Rate (Gbps)	3.08	1.37	0.026
Min-Entropy per 8 bits	7.897	7.902	7.890
IID Test[36]	Pass	Pass	Pass
Randomness Test[42]	Pass	Pass	Pass

cal side information E [25, 41]:

$$H_{min}(M_{dis}|E) = -\log_2 \left[\max_{e\in\mathbb{R}} \max_{m_i \in M_{dis}} P_{M_{dis}|E}(m_i|e) \right] \quad (1)$$

where m_i and e are the samples from their respective distributions. Taking a maximum classical noise spread of $e_{max} = 5\sigma_E$, and using a representative sample of 1×10^6 samples per channel we numerically evaluate Equation 1 and find a worse case min entropy of $H_{min}(M_{dis}|E) \geq 9.201$ across all seven channels, 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 [43] 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 (A) 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. This extractor is designed to minimise the effect of the classical noise on the output signal. The total bit rate of this construction is given by the product of the sample rate (55MSPS), extracted bits per sample (8), and number

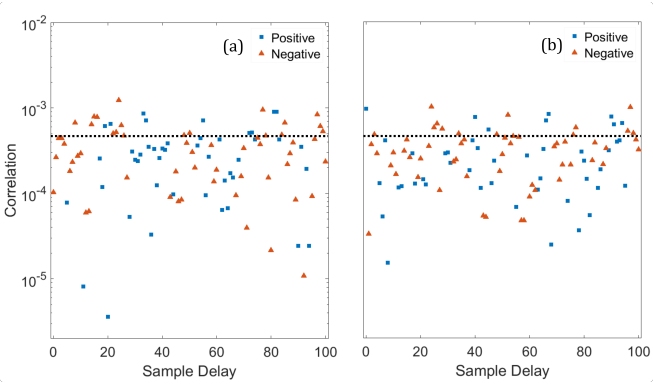

Figure 3: Correlation between the output of a single two-source extractor and its inputs 1(a) and 2(b). Both positive (squares) and negative (triangles) correlations are plotted, with the y-axis shared between plots. The black dotted line represents the correlation of perfectly random data for the sample size, 4.8×10^{-4}.

of channels (7), and is 3.08 Gbit/s. We sample at least 27.5 MHz of the homodyne detector bandwidth as allowed by the Shannon-Hartley limit[8]. The sampling rate is limited by the interface between the ADC and FPGA. 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 [25], 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 vetted 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. Whilst the output bit rate is much lower because it requires two 36 bit inputs (72 raw bits total) to produce one output bit, it removes the necessity for an externally generated seed, prevalent in most QRNG demonstrations. 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 7×10^8 bits and find extraction methods A, B, and C pass all tests.

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 4.3×10^6 samples. The

theoretical correlation of perfectly random data for the sample size is 4.8×10^{-4}.

4 Conclusion

In summary, we have demonstrated a high-speed 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, and to supply 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(C) 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.

The highly specialized nature of the optical and electronic components makes a system on a single circuit board the realistic short-term integration option for GHz rate QRNG. To continue the scaling of this system to hundreds of channels full integration of a high power 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 [44]. The simplicity of the entropy source makes quantum vacuum fluctuations an excellent choice for parallelisation with Gbps single channel bitrates reported.

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 research is financially supported by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (CE170100012) and the Griffith University Research Infrastructure Programme.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.

References

[1] W. H. Ware, in *Proceedings of the Spring Joint Computer Conference* (1967) pp. 279–282.

[2] P. Zhang, K. Aungskunsiri, E. Martín-López, J. Wabnig, M. Lobino, R. W. Nock, J. Munns, D. Bonneau, P. Jiang, H. W. Li, A. Laing, J. G. Rarity, A. O. Niskanen, M. G. Thompson, and J. L. O'Brien, Physical Review Letters **112**, 130501 (2014).

[3] Debian, *Debian - Security Information - DSA-1571-1 openssl*, https://www.debian.org/security/2008/dsa-1571.

[4] L. Dorrendorf, Z. Gutterman, and B. Pinkas, ACM Transactions on Information and System Security **13**, 1 (2009).

[5] K. Nohl, D. Evans, Starbug, and H. Plotz, in *17th USENIX Security Symposium* (2008) pp. 185–193.

[6] M. Herrero-Collantes and J. C. Garcia-Escartin, Reviews of Modern Physics **89**, 1 (2017).

[7] X. Ma, X. Yuan, B. Qi, and Z. Zhang, npj Quantum Information **221**, 1 (2016).

[8] J. D. Hart, Y. Terashima, A. Uchida, G. B. Baumgartner, T. E. Murphy, and R. Roy, APL Photonics **2**, 1 (2017).

[9] Y. Q. Nie, J. Y. Guan, H. Zhou, Q. Zhang, X. Ma, and J. W. Pan, Physical Review A **94**, 060301 (2016).

[10] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature **464**, 1021 (2010).

[11] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, A. K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm, (2017), arXiv 1702.05178.

[12] A. Kulikov, M. Jerger, A. Potočnik, A. Wallraff, and A. Fedorov, Physical Review Letters **119**, 240501 (2017).

[13] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil, Physical Review A **86**, 062109 (2012).

[14] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Physical Review Letters **120**, 010503 (2018).

[15] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquadt, and G. Leuchs, Nature Photonics **4**, 711 (2010).

[16] L. Li, A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang, IEEE Photonics Journal **6** (2014), 10.1109/JPHOT.2014.2304555.

[17] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Physical Review Letters **114**, 150501 (2015).

[18] M. W. Mitchell, C. Abellan, and W. Amaya, Physical Review A **91**, 012314 (2015).

[19] D. G. Marangon, G. Vallone, and P. Villoresi, Physical Review Letters **118**, 060503 (2017).

[20] M. Virte, E. Mercier, H. Thienpont, K. Panajotov, and M. Sciamanna, Optics Express **22**, 17271 (2014).
[21] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, Journal of Modern Optics **56**, 516 (2009).
[22] F. Xu, B. Qi, X. Ma, H. Zheng, and H. K. Lo, Optics Express **20**, 12366 (2012).
[23] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, Optics Express **23**, 1470 (2015).
[24] M. Gräfe, R. Heilmann, A. Perez-Leija, R. Keil, F. Dreisow, M. Heinrich, H. Moya-Cessa, S. Nolte, D. N. Christodoulides, and A. Szameit, Nature Photonics **8**, 791 (2014).
[25] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Physical Review Applied **3**, 054004 (2015).
[26] IDQuantique, *Quantis QRNG Brochure*, https://www.idquantique.com (2016).
[27] R. Shaltiel, in *Lecture Notes in Computer Science*, Vol. 6756 (2011) pp. 21–41.
[28] R. Kasher and J. Kempe, in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, Lecture Notes in Computer Science, Vol. 6302, pp. 656–669.
[29] K. Ugajin, Y. Terashima, K. Iwakawa, A. Uchida, T. Harayama, K. Yoshimura, and M. Inubushi, Optics Express **25**, 6511 (2017).
[30] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, J. Zhang, and J.-W. Pan, Review of Scientific Instruments **87**, 076102 (2016).
[31] D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. J. Shields, Journal of Lightwave Technology **36**, 3778 (2018).
[32] Y. Shen, L. Tian, and H. Zou, Physical Review A **81**, 063814 (2010).
[33] R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. H. Huntington, and A. I. Lvovsky, Optics Communications **285**, 24 (2012).
[34] F. Lenzini, S. Kasture, B. Haylock, and M. Lobino, Optics Express **23**, 1748 (2015).
[35] T. Symul, S. M. Assad, and P. K. Lam, Applied Physics Letters **98**, 23 (2011).
[36] M. Sönmez Turan, E. Barker, J. Kelsey, M. Boyle, M. Kerry, and M. L. Baish, *"Recommendation for the Entropy Sources Used for Random Bit Generation (Second DRAFT) NIST Special Publication 800-90B*, National Institute of Standards and Technology (2016).
[37] M. Dworkin, *Recommendation for Block Cipher Mode of Operation: The CMAC Mode for Authentication. NIST Special Publication 800-38B*, National Institute of Standards and Technology (2005).
[38] *Specification for the Advanced Encryption Standard (AES) FIPS 197*, National Institute of Standards and Technology (2001).
[39] H. Hsing, *AES :: Overview :: OpenCores*, https://opencores.org/project/tiny_aes.
[40] J. Bouda, M. Pivoluska, and M. Plesch, Theoretical Computer Science **459**, 69 (2012).
[41] R. Renner, International Journal of Quantum Information **6**, 1 (2008).
[42] A. Rukhin, J. Soto, J. Nechvatal, S. Miles, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Rev. 1a*, National Institute of Standards and Technology (2010).
[43] K. McKay and J. Kelsey, *GitHub - usnistgov/SP800-90B _EntropyAssessment*, https://github.com/usnistgov/SP800-90B_EntropyAssessment.
[44] J. W. Silverstone, D. Bonneau, J. L. O'Brien, and M. G. Thompson, IEEE Journal of Selected Topics in Quantum Electronics **22**, 390 (2016).