Random number generation from spontaneous Raman scattering

M. J. Collins, A. S. Clark, C. Xiong, E. Mägi, M. J. Steel, and B. J. Eggleton

Citation: Applied Physics Letters **107**, 141112 (2015); doi: 10.1063/1.4931779
View online: http://dx.doi.org/10.1063/1.4931779
View Table of Contents: http://scitation.aip.org/content/aip/journal/apl/107/14?ver=pdfcov
Published by the AIP Publishing

Random number generation from spontaneous Raman scattering

M. J. Collins,[1,a)] A. S. Clark,[1,2] C. Xiong,[1] E. Mägi,[1] M. J. Steel,[3] and B. J. Eggleton[1]
[1]*ARC Centre of Excellence for Ultrahigh bandwidth Devices for Optical Systems (CUDOS), Institute of Photonics and Optical Science (IPOS), School of Physics, University of Sydney, New South Wales 2006, Australia*
[2]*Centre for Cold Matter, Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom*
[3]*CUDOS, MQ Photonics Research Centre, Department of Physics and Astronomy, Macquarie University, New South Wales 2109, Australia*

(Received 16 April 2015; accepted 6 September 2015; published online 9 October 2015)

We investigate the generation of random numbers via the quantum process of spontaneous Raman scattering. Spontaneous Raman photons are produced by illuminating a highly nonlinear chalcogenide glass (As_2S_3) fiber with a CW laser at a power well below the stimulated Raman threshold. Single Raman photons are collected and separated into two discrete wavelength detuning bins of equal scattering probability. The sequence of photon detection clicks is converted into a random bit stream. Postprocessing is applied to remove detector bias, resulting in a final bit rate of ~650 kb/s. The collected random bit-sequences pass the NIST statistical test suite for one hundred 1 Mb samples, with the significance level set to $\alpha = 0.01$. The fiber is stable, robust and the high nonlinearity (compared to silica) allows for a short fiber length and low pump power favourable for real world application. © *2015 AIP Publishing LLC*.
[http://dx.doi.org/10.1063/1.4931779]

Randomness is a vital resource for many modern cryptographic systems, quantum communication,[1] statistical data analysis,[2] and Monte-Carlo simulations. Pseudo-random number generators (PRNG) are currently used for the majority of these applications, deterministically generating bit-sequences that appear random. PRNG algorithms invariably require a seed to initiate a particular sequence. In contrast, true random number generators (TRNG) are based on physical phenomena which are fundamentally non-deterministic. TRNG devices act as an interface between physical randomness and the digital world and can function as a seed for a PRNG. PRNGs often produce random numbers with better statistics and at a faster rate than TRNGs, which may suffer from technical implementation challenges and physical biases, creating a synergy between the two technologies.

Quantum mechanical indeterminacy presents an obvious source of physical randomness. If the source of randomness for a TRNG is quantum-mechanical the device is called a quantum random number generator (QRNG). Some examples of quantum optical measurements used for randomness generation include the timing of neutron emissions from radioactive material,[3,4] detection of a single photon at the output ports of a beam-splitter,[5–8] the phase or intensity of a nonlinear pulse in a stimulated Raman scattering (SRS) experiment[9–11] or laser[12] and photon number detection statistics.[13,14]

Another source of quantum noise fluctuations is spontaneous Raman scattering (SpRS).[15] SpRS occurs when a photon is scattered spontaneously by the interaction with a crystal or amorphous lattice to create/absorb a phonon with a corresponding red/blue shift in the photon frequency. These are called Stokes and anti-Stokes events, respectively. The Stokes case is illustrated in Fig. 1(a). For large frequency shifts, where the population of the thermal phonon field is negligible, scattering is dominated by the interaction between the incident light and quantum mechanical vacuum phonon fluctuations. SpRS is normally considered a nuisance in nonlinear quantum photonics, notably in the context of heralded single photon generation.[16,17] This is especially so for amorphous materials, for which the spontaneous Raman spectrum is very broad, typically spanning 10 THz or so. Nevertheless, since the timing and frequency of detected

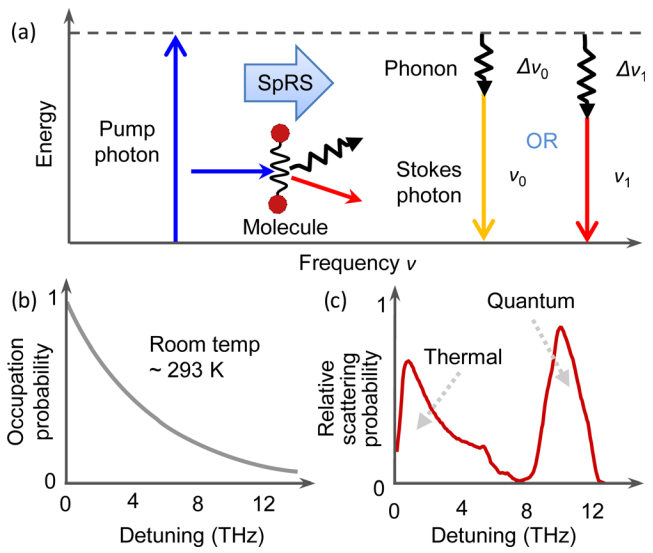

FIG. 1. (a) Energy diagram for the Stokes SpRS process. A pump photon scatters to generate a phonon and a red-shifted photon with random detuning from the pump $\Delta\nu$. (b) The Bose-Einstein phonon population distribution at room temperature (293 K). (c) Scattering probability distribution for SpRS. Lower energy thermal phonon states are more likely to be occupied, thereby enhancing the SpRS close to the pump. Larger shifts are due predominantly to scattering from quantum noise phonons.

a)mcoll@physics.usyd.edu.au

spontaneous Raman photons is unpredictable, here we harness the process as a useful resource for randomness.

We describe a QRNG based on SpRS in a highly nonlinear As_2S_3 glass fiber. The high nonlinearity allows for a short length of fiber to be used with pump powers available from commercial fiber lasers. The smaller Raman shift in As_2S_3 compared with standard silica glass allows the pump light and Raman photons to both sit in the telecommunications S and C bands where fiber-based pump sources and filters are commercially available. In addition, the fiber form factor is robust and readily packaged for real world applications. Here, we measured a raw bit rate of 1.00 Mb/s with a post processed bit rate of ~650 kb/s. Our SpRS-QRNG passed the NIST statistical randomness tests, an industry standard for evaluating PRNG and TRNG technology.[18]

As a spontaneous phenomenon, the likelihood of a SpRS event scales linearly with the strength of the input field.[19] The frequency dependence of the density of phonon states $\rho_{\mathrm{ph}}(\nu)$ is characteristic for any material as is the measurable scattered Raman spectrum. Indeed $\rho_{\mathrm{ph}}(\nu)$ is related to the nonlinear Raman gain as $g(\nu) \propto \frac{1}{\nu}\rho_{\mathrm{ph}}(\nu)$, with ν the frequency shift from the pump. In an amorphous, isotropic material the Raman scattering spectrum contains both an *isotropic* and an *anisotropic* component,[20,21] resulting in a polarization dependence in the SpRS spectrum. For weak illumination, the expected detection rate of SpRS photons is[21,22]

$$R_{\mathrm{SpRS}}(\nu, T) = C\eta\Delta\nu PL\,[\,1 + n_{\mathrm{BE}}(\nu, T)\,]\,g(\nu), \qquad (1)$$

where C is the Raman coupling coefficient, η is an experimental loss factor, $\Delta\nu$ is the measurement bandwidth, P is the CW laser power, L is the effective scattering device length, and $g(\nu)$ is the gain profile which includes the contribution of both polarization components.

The factor $n_{\mathrm{BE}}(\nu, T)$ is the Bose-Einstein thermal photon occupation number

$$n_{\mathrm{BE}}(\nu, T) = \frac{1}{e^{\frac{h\nu}{k_B T}} - 1}, \qquad (2)$$

where $k_B T$ is the thermal energy and $h\nu$ is the phonon energy. n_{BE} describes the probability a state is occupied by a thermal phonon, shown in Fig. 1(b). As the phonon energy increases, the likelihood of a phonon state being occupied decreases. In the regime of small Raman shift and low energy phonons, SpRS events are predominantly scattering from thermal phonons. However for large Raman shifts, the thermal occupation of phonon states approaches zero, and SpRS events are dominated by scattering from quantum fluctuations in the phonon field. The two regimes are marked in the SpRS spectrum[23] shown in Fig. 1(c). For As_2S_3 chalcogenide the peak of the SpRS scattering spectrum lies at ~10.4 THz. At room temperature the contribution of SpRS from thermal scattering events at this detuning is ~18%.

Operating in the regime of large pump detuning, random bit-sequences were generated using the following procedure. Single photons from the pump were scattered randomly into one of two frequency bins labeled ν_0 and ν_1, detected using single photon detectors (SPDs). The detected photon rate was 500 kHz each for channels 0 and 1 at an input pump power of 550 μW. The combined collection and detection efficiency of −20 dB implies an in-fiber generation rate of 100 MHz for photons within channels ν_0 and ν_1. The temporal sequence of the photon detection generates the random bit-string. This discrete detection of SpRS single-photons, generated with random frequency, differs significantly compared to the SRS based QRNG demonstrations.[9–11] The SRS approaches rely on phase/intensity variations of a spontaneously initiated light beam amplified by stimulated Raman scattering with digital conversion of an analogue measurement required to generate a bit-string.

Figure 2 outlines the experimental layout of the SpRS-QRNG. A Keopsys CW laser centered at 1480 nm was used to pump a 24 cm piece of As_2S_3 highly nonlinear chalcogenide glass fiber with a nonlinearity parameter $\gamma = 1.7$ $W^{-1}m^{-1}$,[24] refractive index 2.44, and transmission loss of 1 dBm^{-1}. The high nonlinearity of this and other chalcogenides makes this QRNG technique potentially compatible with planar photonic chip integration.[25] The fiber was made from a multi-mode sample (CorActive) with a core diameter of 5.0 μm that was tapered to 2.9 μm for single mode operation, using a soft-glass fiber tapering rig.[26] The fiber was butt-coupled and UV-cure glued (glue refractive index 1.76) directly to high numerical aperture silica fibers (refractive index 1.44) to minimize the mode mismatch and reduce Fresnel reflections. The high numerical aperture (high-NA) fiber was then fusion-spliced to standard single mode SMF28 silica fiber pigtails with FC/APC connectors. To check for any SpRS contribution from the silica pigtails, the chalcogenide was bypassed resulting in a negligible increase in the photons counts above the noise (i.e., the dark count rate with no input to the detectors). This is as expected as the nonlinear coefficient of chalcogenide is 100× larger than the high-NA fiber ($\gamma \sim 2 \times 10^{-2}$ $W^{-1}m^{-1}$) and 1000× larger

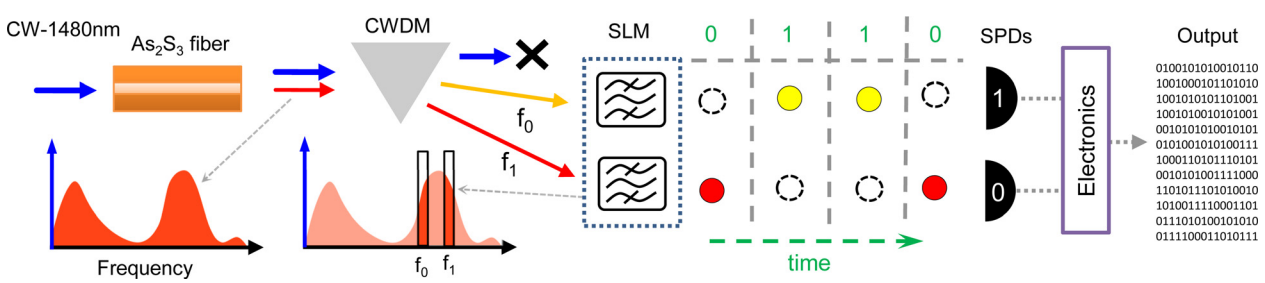

FIG. 2. The conceptual illustration of the SpRS based QRNG. A CW laser at 1480 nm pumps a chalcogenide fiber to generate SpRS photons. A CDWM drops the pump and a SLM is used to define two discrete frequency bins. SPDs detect the SpRS photons, with the two bins labeled "0" and "1," respectively. The time sequence of the photon detection generates a random bit-string at the output.

than the standard fiber ($\gamma \sim 2 \times 10^{-3}$ $W^{-1}m^{-1}$),[25] and we kept both fibers short at 0.1 m and 0.3 m, respectively.

The pump and the SpRS photons leaving the fiber were wavelength separated using a coarse wavelength division multiplexer (CWDM). The pump channel was dropped and the Raman photons in the range 1561 nm ± 6.5 nm were passed. A liquid crystal on silicon based spatial light modulator (SLM—Finisar Waveshaper) was configured to define two discrete frequency-bins each with 125 GHz bandwidth, centered at $\nu_0 = 192.245$ THz (∼1559.4 nm) and $\nu_1 = 191.63$ THz (∼1564.4 nm), respectively. Superconducting single photon detectors (SPDs—Single Quantum) were placed at the output of each fiber channel ν_0 and ν_1 and the detection events were electronically time-tagged. The detector efficiency was ∼15% with a dark count rate of ∼100 Hz. By adjusting the attenuation of channel 0 by ~ -0.8 dB, the photon detection rate on each channel was balanced to within ±1 kHz. A 0 or 1 bit was added to the bit-sequence for each sequential detector click on channel ν_0 or ν_1, respectively. Simultaneous detections on both bin channels were ignored. To test the performance of the SpRS-QRNG, one hundred samples of 1 Mb were recorded and evaluated using the NIST tests.

A bias towards either 0 or 1 can be expected in the raw bit-sequence due to both differences in the collection efficiencies of the two detector channels and the non-flatness of the Raman spectrum. To reduce this bias, a simple post-processing XOR operation was performed with a 16-bit delayed copy of the raw sequence. This reduced the raw bit rate of 1.00 Mb/s to the final post-processed bit rate of ∼650 kb/s. At this bit rate our SpRS-QRNG passed all of the NIST statistical randomness tests.[18] The results of the 14 standard tests listed in Table I.

The theoretical maximum bit rate limit follows from the decay time of the Raman response function,[29] which is ∼100 fs for As_2S_3. If SpRS photons are generated successively on a time scale faster than the Raman response time this can introduce frequency correlations. To guarantee no correlation, the probability of generating two photons within a 100 fs window must be kept low. In our case, on average one photon is generated every 10 ns (corresponding to a 100 MHz in-fiber generation rate). Assuming a Poisson distribution for the photon generation[30] the probability of generating two photons within 100 fs is $\sim 5.0 \times 10^{-5}$, confirming the device is operating below the stimulated Raman threshold in the single-photon regime. Increasing the in-fiber generation rate to 1 GHz, this two photon probability remains low at $\sim 5.0 \times 10^{-3}$.

For this experiment, the maximum rate was limited by detection and collection efficiency and detector saturation levels. Higher bit rates could be obtained with improved photon detector technology, which has already reached the GHz regime with solid state detectors at telecommunication wavelengths[28] or alternatively by operating in the visible regime, where silicon-based photon detectors have much higher efficiencies. In addition the scheme is scalable to multiple channels across the 3 THz bandwidth of the As_2S_3 Raman peak,[23,24] beyond which SpRS photons are inefficiently generated in the desired large detuning regime. Scaling to multiple detection channels can be done using commercial wavelength division components such as arrayed waveguide gratings. To scale up a QRNG system based on an attenuated laser incident on a beam-splitter,[5–8] assuming the limitation is detector efficiency, would require an expensive custom beam-splitter circuit to implement. Detector improvements, or multiplexing many slower frequency channel pairs across the whole Raman peak, both offer a clear route to orders of magnitude higher bit rates.

In conclusion, we have demonstrated a quantum random number generator with a bit rate of ∼650 kb/s (raw bit rate of 1.00 Mb/s) by frequency binning SpRS photons from an As_2S_3 chalcogenide glass fiber. The high nonlinearity allowed a short piece of fiber to be used with modest pump powers. The output bit-sequences all passed the NIST suite of randomness tests at a significance level of 0.01. This scheme has the potential for random number generation at Gigabit per second rates by either moving to faster single photon detectors,[28] or by wavelength division multiplexing of a number of channel pairs.

TABLE I. Results of NIST statistical randomness test suite, using 100 samples of 1 Mb and significance level $\alpha = 0.01$. For the test to be considered passed the *P-value* $_T$ (Uniformity of the P-value distribution) should be greater than 0.0001 and the proportions greater than 0.96 (or ∼0.95 where appropriate). For the tests that produce multiple *P-values* $_T$ values the worst (lowest) value, and corresponding proportion, was tabulated.[18]

Test name	*P-value* $_T$	Proportion	Result
Frequency	0.162606	0.99	Pass
Block frequency	0.181557	0.98	Pass
Cumulative sums	0.04872	0.99	Pass
Runs	0.350485	0.97	Pass
Longest run	0.030806	1.00	Pass
Rank	0.401199	1.00	Pass
Non-overlapping template	0.000648	0.97	Pass
Overlapping template	0.998821	0.99	Pass
Universal	0.699313	0.99	Pass
Approximate entropy	0.719747	0.99	Pass
Random excursions	0.178278	0.983 (Ref. 27)	Pass
Random excursions variant	0.01125	1.00 (Ref. 27)	Pass
Serial	0.213309	1.00	Pass
Linear complexity	0.534146	0.98	Pass

This work was supported by the Centre of Excellence (CUDOS, Project No. CE110001018), the Laureate Fellowship (FL120100029), and the Discovery Early Career Researcher Award Programs (DE130101148 and DE120100226) of the Australian Research Council (ARC).

[1]N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2]S. L. Lohr, *Sampling: Design and Analysis* (Springer, 2010).
[3]M. Gude, Frequenz **39**, 187 (1985).
[4]M. P. Silverman, W. Strange, C. Silverman, and T. C. Lipscombe, Phys. Rev. A **61**, 042106 (2000).
[5]J. Rarity, P. Owens, and P. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[6]A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[7]T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[8]P. Bronner, A. Strunz, C. Silberhorn, and J.-P. Meyn, Eur. J. Phys. **30**, 1189 (2009).

[9]P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, Opt. Express **19**, 25173 (2011).
[10]P. J. Bustard, D. G. England, J. Nunn, D. Moffatt, M. Spanner, R. Lausten, and B. J. Sussman, Opt. Express **21**, 29350 (2013).
[11]D. G. England, P. J. Bustard, D. J. Moffatt, J. Nunn, R. Lausten, and B. J. Sussman, Appl. Phys. Lett. **104**, 051117 (2014).
[12]H. Guo, W. Tang, Y. Liu, and W. Wei, Phys. Rev. E **81**, 051137 (2010).
[13]J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).
[14]W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).
[15]R. Boyd, *Nonlinear Optics*, 3rd ed. (Springer, 1992).
[16]K. Inoue and K. Shimizu, Jpn. J. Appl. Phys., Part 1 **43**, 8048 (2004).
[17]A. S. Clark, M. J. Collins, A. C. Judge, E. C. Mägi, C. Xiong, and B. J. Eggleton, Opt. Express **20**, 16807 (2012).
[18]A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *NIST Special Publication 800-22, Revision 1-a* (NIST, Gaithersburg, Maryland, USA, 2010).
[19]G. P. Agrawal, *Nonlinear Fiber Optics*, 4th ed. (Springer, 2007).
[20]R. Hellwarth, J. Cherlow, and T.-T. Yang, Phys. Rev. B **11**, 964 (1975).
[21]Q. Lin, F. Yaman, and G. Agrawal, Phys. Rev. A **75**, 023803 (2007).
[22]R. Kobliska and S. Solin, Phys. Rev. B **8**, 756 (1973).
[23]M. J. Collins, A. C. Judge, A. S. Clark, S. Shahnia, E. C. Magi, M. J. Steel, C. Xiong, and B. J. Eggleton, Appl. Phys. Lett. **101**, 211110 (2012).
[24]C. Xiong, E. Mägi, F. Luan, A. Tuniz, S. Dekker, J. S. Sanghera, L. B. Shaw, I. D. Aggarwal, and B. J. Eggleton, Appl. Opt. **48**, 5467 (2009).
[25]B. J. Eggleton, B. Luther-Davies, and K. Richardson, Nat. Photon. **5**, 141 (2011).
[26]E. C. Mägi, L. B. Fu, H. C. Nguyen, M. R. Lamont, D. I. Yeom, and B. J. Eggleton, Opt. Express **15**, 10324 (2007).
[27]Only 60 samples used in test with a pass proportion of 0.95.
[28]Z. L. Yuan, B. E. Kardynal, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **91**, 041114 (2007).
[29]M. Asobe, T. Kanamori, K. Naganuma, H. Itoh, and T. Kaino, J. Appl. Phys. **77**, 5518 (1995).
[30]H. Takesue and K. Shimizu, Opt. Commun. **283**, 276 (2010).