Quantum random bit generation using energy fluctuations in stimulated Raman scattering

Philip J. Bustard,[1] Duncan G. England,[1] Josh Nunn,[1,2] Doug Moffatt,[1] Michael Spanner,[1] Rune Lausten,[1] and Benjamin J. Sussman[1,2]*

[1]*National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario, K1A 0R6, Canada*
[2]*Department of Physics, University of Ottawa, Ottawa, Ontario, K1N 6N5, Canada*

**ben.sussman@nrc.ca*

http://quantumtechnology.ca/

Abstract: Random number sequences are a critical resource in modern information processing systems, with applications in cryptography, numerical simulation, and data sampling. We introduce a quantum random number generator based on the measurement of pulse energy quantum fluctuations in Stokes light generated by spontaneously-initiated stimulated Raman scattering. Bright Stokes pulse energy fluctuations up to five times the mean energy are measured with fast photodiodes and converted to unbiased random binary strings. Since the pulse energy is a continuous variable, multiple bits can be extracted from a single measurement. Our approach can be generalized to a wide range of Raman active materials; here we demonstrate a prototype using the optical phonon line in bulk diamond.

OCIS codes: (190.5650) Raman effect; (190.5890) Scattering, stimulated; (290.5910) Scattering, stimulated Raman; (270.2500) Fluctuations, relaxations, and noise; (030.6600) Statistical optics; (270.1670) Coherent optical effects.

References and links

1. B. Hayes, "Randomness as a resource," Am. Sci. **89**, 300–304 (2001).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
3. S. L. Lohr, *Sampling: Design and Analysis* (Cengage Learning, 2010).
4. N. Metropolis and S. Ulam, "The Monte Carlo method," J. Am. Stat. Assoc. **44**, 335–341 (1949).
5. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Opt. **47**, 595–598 (2000).
6. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**, 711–715 (2010).
7. Y. Shen, L. Tian, and H. Zou, "Practical quantum random number generator based on measuring the shot noise of vacuum states," Phys. Rev. A **81**, 063814 (2010).
8. T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett. **98**, 231103 (2011).
9. B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**, 312–314 (2010).
10. H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," Phys. Rev. E **81**, 051137 (2010).
11. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," Opt. Express **19**, 20665–20672 (2011).

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

12. F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**, 12366–12377 (2012).
13. A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, "All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators," Opt. Express **20**, 19322–19330 (2012).
14. S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, "Random numbers certified by Bell's theorem," Nature **464**, 1021–1024 (2010).
15. M. Um, X. Zhang, J. Zhang, Y. Wang, S. Yangchao, D.-L. Deng, L.-M. Duan, and K. Kim, "Experimental certification of random numbers via quantum contextuality," Sci. Rep. **3**, 1627 (2013).
16. J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," Appl. Phys. Lett. **93**, 031109 (2008).
17. W. Wei and H. Guo, "Bias-free true random-number generator," Opt. Lett. **34**, 1876–1878 (2009).
18. M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," Opt. Express **18**, 13029–13037 (2010).
19. M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," Phys. Rev. A **83**, 023820 (2011).
20. M. Wahl, M. Leifgen, M. Berlin, T. Röhlicke, H.-J. Rahn, and O. Benson, "An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements," Appl. Phys. Lett. **98**, 171105 (2011).
21. H. Schmidt, "Quantum mechanical random number generator," J. Appl. Phys. **41**, 462–468 (1970).
22. P. J. Bustard, D. Moffatt, R. Lausten, G. Wu, I. A. Walmsley, and B. J. Sussman, "Quantum random bit generation using stimulated Raman scattering," Opt. Express **19**, 25173–25180 (2011).
23. H. Krawczyk, "LFSR-based hashing and authentication," in "Advances in Cryptology - CRYPTO'94," , vol. 839 of *Lecture Notes in Computer Science*, Y. Desmedt, ed. (Springer, 1994), pp. 129–139.
24. X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, "Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction," Phys. Rev. A **87**, 062327 (2013).
25. A. Penzkofer, A. Laubereau, and W. Kaiser, "High intensity Raman interactions," Prog. Quantum Electron. **6**, 55–140 (1979).
26. M. G. Raymer and J. Mostowski, "Stimulated Raman scattering: unified treatment of spontaneous initiation and spatial propagation," Phys. Rev. A **24**, 1980–1993 (1981).
27. S. J. Kuo, D. T. Smithey, and M. G. Raymer, "Spatial interference of macroscopic light fields from independent Raman sources," Phys. Rev. A **43**, 4083–4086 (1991).
28. D. T. Smithey, M. Belsley, K. Wedding, and M. G. Raymer, "Near quantum-limited phase memory in a Raman amplifier," Phys. Rev. Lett. **67**, 2446–2449 (1991).
29. M. Belsley, D. T. Smithey, K. Wedding, and M. G. Raymer, "Observation of extreme sensitivity to induced molecular coherence in stimulated Raman scattering," Phys. Rev. A **48**, 1514–1525 (1993).
30. M. G. Raymer, K. Rzążewski, and J. Mostowski, "Pulse-energy statistics in stimulated Raman scattering," Opt. Lett. **7**, 71–73 (1982).
31. I. A. Walmsley and M. G. Raymer, "Observation of macroscopic quantum fluctuations in stimulated Raman scattering," Phys. Rev. Lett. **50**, 962–965 (1983).
32. I. A. Walmsley and M. G. Raymer, "Experimental study of the macroscopic quantum fluctuations of partially coherent stimulated Raman scattering," Phys. Rev. A **33**, 382–390 (1986).
33. J. Mostowski and B. d. z. Sobolewska, "Transverse effects in stimulated Raman scattering," Phys. Rev. A **30**, 610–612 (1984).
34. M. G. Raymer, I. A. Walmsley, J. Mostowski, and B. Sobolewska, "Quantum theory of spatial and temporal coherence properties of stimulated Raman scattering," Phys. Rev. A **32**, 332–344 (1985).
35. F. C. Waldermann, B. J. Sussman, J. Nunn, V. O. Lorenz, K. C. Lee, K. Surmacz, K. H. Lee, D. Jaksch, I. A. Walmsley, P. Spizziri, P. Olivero, and S. Prawer, "Measuring phonon dephasing with ultrafast pulses using Raman spectral interference," Phys. Rev. B **78**, 155201 (2008).
36. K. C. Lee, B. J. Sussman, J. Nunn, V. O. Lorenz, K. Reim, D. Jaksch, I. A. Walmsley, P. Spizzirri, and S. Prawer, "Comparing phonon dephasing lifetimes in diamond using transient coherent ultrafast phonon spectroscopy," Diamond Relat. Mater. **19**, 1289–1295 (2010).
37. K. C. Lee, B. J. Sussman, M. R. Sprague, P. Michelberger, K. F. Reim, J. Nunn, N. K. Langford, P. J. Bustard, D. Jaksch, and I. A. Walmsley, "Macroscopic non-classical states and terahertz quantum processing in room-temperature diamond," Nat. Photonics **6**, 41–44 (2011).
38. K. Rzążewski, M. Lewenstein, and M. G. Raymer, "Statistics of stimulated Stokes pulse energies in the steady-state regime," Opt. Commun. **43**, 451–454 (1982).
39. G. Marsaglia, "Diehard battery of tests of randomness," www.stat.fsu.edu/pub/diehard/ (1995).
40. J. Reintjes and M. Bashkansky, *Handbook of Optics, Volume IV: Optical Properties of Materials, Nonlinear Optics, Quantum Optics*, 3rd ed. (McGraw-Hill Professional, 2010), Chap. 15, p. 15.1.
41. F. Benabid, J. C. Knight, G. Antonopoulos, and P. S. J. Russell, "Stimulated Raman scattering in hydrogen-filled hollow-core photonic crystal fiber," Science **298**, 399–402 (2002).

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

1. Introduction

Random bit strings are of great utility in modern information processing systems [1]. They are used in cryptography [2], statistical sampling [3], and Monte Carlo simulations [4]. However, the generation of truly random bit strings remains a non-trivial problem. Most methods in use today are pseudo-random. With sufficient processing power, or knowledge of the generation technique, the output of a pseudo-random number generator may become predictable, which can lead to undesirable computational failures or security breaches.

Quantum random number generation (QRNG) techniques offer a robust alternative to pseudo-random methods. These methods rely on the inherently probabilistic outcomes of measurements on suitable quantum systems: while the probabilities of a measurement result may be accurately predicted by quantum theory, the outcome of a given measurement is random for a suitably prepared state. Example QRNG sources include beam splitter partition noise for photons [5], the shot noise of vacuum states [6–8], laser phase noise [9–12], binary phase fluctuations in a parametric oscillator [13], fluorescence from entangled ions [14, 15], photon statistics [16–20], and radioactive decay [21]. We recently demonstrated that random numbers can be generated by measuring the phase of Stokes light produced using spontaneously-initiated stimulated Raman scattering (SISRS) [22]. In this letter, we use the pulse energy fluctuations of Stokes light from SISRS as a source of randomness for QRNG. We convert measured Stokes pulse energies to strings of unbiased random bits using a random Toeplitz matrix to implement a randomness extractor [23, 24]. The use of SISRS energy fluctuations rather than SISRS phase noise for QRNG [22] enables a simpler detection setup that does not require an interferometer and reference pulse with which to measure the target quantum random variable. Instead, energy fluctuations are easily measured with high signal-to-noise ratio using fast, inexpensive detectors such as PIN photodiodes, making them a convenient source of entropy for QRNG; this simple detection setup can readily be scaled to higher repetition rates.

Raman scattering is the inelastic scattering of photons from vibrational, rotational, or electronic excitations in the Raman-active medium. Here we use Raman scattering in diamond, as shown in Fig. 1. The population is initially in the the ground state, and the excited state is the optical phonon branch. In a typical Raman scattering event, an incoming 'pump' photon is annhilated, and a red-shifted 'Stokes' photon is created; the remaining energy is transferred to the diamond as an optical phonon. We focus a strong pump pulse through a diamond sample with no input Stokes pulse and no pre-existing excitation in the medium. Stokes photons scattered spontaneously into the path of the pump pulse stimulate more scattering events so that

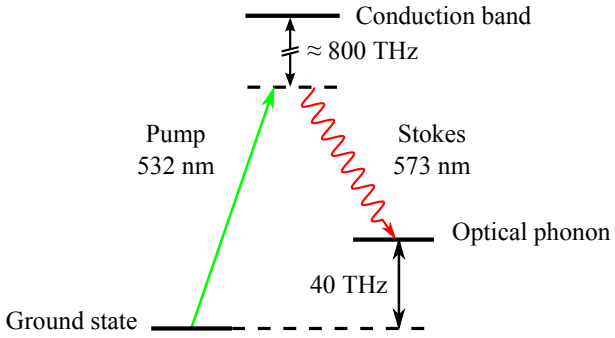

Fig. 1. Λ-level diagram for Stokes Raman scattering in diamond. Inelastic scattering annihilates the pump photon at 532 nm, creating an optical phonon in the diamond and a red-shifted Stokes photon at 573 nm.

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

the Stokes pulse grows by stimulated Raman scattering as it propagates through the diamond. Spontaneous Raman scattering is a quantum phenomenon caused by pump photons scattering from broadband vacuum fluctuations of the electromagnetic field [25, 26]. The quantum mechanical origin of the Stokes pulse is manifest in its statistics, with large fluctuations in both phase [27–29] and energy [30–34].

Our technique has the potential to generate very high bit-rates with rapid turn-on times because the non-resonant nature of the Raman interaction allows broad-bandwidth, ultrashort pulses to be used and because the rapid decay of the optical phonons promptly resets the vacuum state before each Stokes pulse is generated. Often in coherent optical experiments such rapid decoherence is problematic, but here it is an advantage. Few-ps Raman decay times are typical in bulk solids and liquids, indicating that the physical limit for uncorrelated, repeated energy measurements is hundreds of GHz across a wide range of possible Raman gain media. Furthermore, the Stokes pulse energy is a continuous variable so that a single measurement can generate multiple random bits: a higher precision measurement extracts more bits, up to a physical limit set by the number of photons in the pulse. A lower threshold practical limit is set by noise in the detection system and by the shape of the Stokes pulse energy distribution. Combining the potential repetition rate and the potential bit extraction depth, the estimated physical limit to data rates is in excess of 1 Tbps.

2. Experiment

Diamond is used as the scattering medium in our QRNG device, shown in Fig. 2. Diamond's large Raman gain coefficient and broad transparency range make it an excellent optical material for use with short pulses. It has a face-centered cubic lattice, with two carbon atoms per unit cell. There is a triply degenerate Raman active optical phonon mode with vibrational symmetry $T_{2g}(\Gamma_5^+)$, and with frequency $\Omega = 40\,\mathrm{THz}$. The phonon is an excitation of a collective vibrational mode in which the two sub-lattices of atoms comprising the diamond crystal move relative to one another. Our diamond is mounted on a steel heat sink at $295 \pm 0.5\,\mathrm{K}$. At room temperature ($T = 295\,\mathrm{K}$), thermal excitation of the optical phonon modes is negligible, with a Boltzmann ratio of $\exp(-h\Omega/k_\mathrm{B}T) = 1.5 \times 10^{-3}$ between the optical phonon band and the ground state. The decoherence time of the optical phonons is $\Gamma^{-1} = 7\,\mathrm{ps}$, based on the Raman linewidth and transient coherent ultrafast phonon spectroscopy measurements [35, 36]. Phonon lifetime measurements have a decay rate of $\approx 2\Gamma$, indicating that the decay mechanism in high grade diamonds is almost completely longitudinal, with negligible transverse dephasing [37].

Our laser source is a Nd:YVO_4 slab amplifier operating at 1 kHz, seeded using a Time-Bandwidth GE-100 Nd:YVO_4 80-MHz oscillator; amplified pulses are frequency-doubled

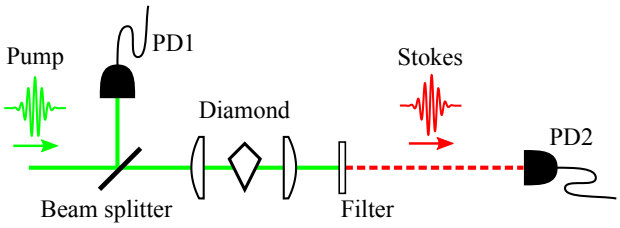

Fig. 2. Experimental setup: the pump pulse is focussed into a diamond plate, generating a Stokes sideband by SISRS. The Stokes pulse is spectrally-filtered from the pump, and its energy is measured by photodiode PD2. Part of the pump pulse energy is separated using a beamsplitter in front of the diamond, and is measured by photodiode PD1.

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

to produce linearly polarized pump pulses with duration $\tau_p = 100\,\text{ps}$, mean pulse energy $W_p \approx 1\,\mu\text{J}$, and wavelength $\lambda_p = 532\,\text{nm}$. Pump pulses are focussed by a 4 cm singlet into a 3 mm synthetic diamond crystal, oriented along the $\langle 100 \rangle$ axis. The pump pulse drives SISRS, generating optical phonons with frequency Ω and correspondingly red-shifted Stokes photons with wavelength $\lambda_S = 573\,\text{nm}$. The product $\Gamma\tau_p \approx 14$ shows that the pump pulse duration is longer than the phonon decay time. Crucially, however, the Raman gain satisfies $gL > \Gamma\tau_p$ where g is the steady-state Raman gain coefficient and L is the effective propagation length; as a result, the SISRS is operating in the transient regime so that the dynamics are coherent and dominated by a single temporal mode [34]. The spatial coherence of the Stokes beam is high because the pump is tightly focussed to a near diffraction-limited spot, with confocal parameter $b \approx 0.2\,\text{mm}$ much shorter than the diamond sample; in this geometry the pump beam effectively acts as a spatial filter for the Stokes light [34]. After generation in the diamond crystal, the Stokes pulse is collimated, and spectrally filtered from the pump using a band-pass filter. The Stokes beam is focussed on to a fast reverse-biased photodiode (PD2; Thorlabs DET10A, Si detector, 1 ns rise time), whose response is electronically integrated using a gated boxcar integrator (Stanford Research Systems SR200); the integrated voltage is digitized using a Measurement Computing USB1608FS data aquisition card and recorded as a Stokes energy measurement W_S with 8 bit resolution.

Our acquisition rate is limited to the pump laser repetition frequency (1 kHz); use of high repetition rate lasers could significantly improve on this practical limitation. The physical limit on the repetition frequency for generation of statistically uncorrelated Stokes pulses is set by the time taken for the number of coherently excited phonons to decay below the quantum noise limit of one phonon per mode. Coherent phonons existing above this level after excitation by a pump pulse would seed scattering from a subsequent pulse, thereby inducing correlations.

The Raman gain is proportional to the pump pulse intensity so energy fluctuations due to laser noise will modify the gain from shot-to-shot. We therefore also partition part of the pump pulse energy using a beam splitter in front of the diamond and detect it with at a fast reverse-biased photodiode (PD1; Thorlabs DET210, Si detector, 1 ns rise time); the photodiode response is digitized using the same procedure as for PD2 and recorded as a reference measurement of the pump pulse energy W_p. The measurements are binned according to pump pulse energy, with each bin of width 0.7% of its mean. This allows us to track and account for the influence of noise from the pump laser on the measured Stokes energy distributions.

Figure 3 shows a typical measured probability distribution $P(W_S|W_p)$ of Stokes energies W_S versus $W_S/\langle W_S \rangle$ for a single pump pulse energy value $W_p = \langle W_p \rangle$, where $\langle \cdot \rangle$ denotes the sample mean. The measured probability distribution plotted in Fig. 3 shows fluctuations in the Stokes pulse energy of up to five times the mean. The shape of the Stokes pulse energy distribution is similar to previous experimental measurements of transient SISRS energy statistics with negligible pump pulse depletion so that the Raman gain is unsaturated [32].

3. Discussion

SISRS is a quantum mechanical process. The Stokes pulse energy is, therefore, a quantum mechanical observable, here denoted by the operator $\widehat{W}_S$. In general, the measured Stokes pulse energy fluctuates from shot-to-shot because of the inherent quantum mechanical uncertainty in SISRS. The shape of the measured statistical distribution of Stokes energies $P(W_S|W_p)$ is determined by the Raman gain, the focussing geometry, and the influence of phonon decay on the scattering process [34]. No general analytic expression is known for the form of $P(W_S|W_p)$. However, in the strongly transient regime with $\Gamma\tau_p = 0$ and unsaturated Raman gain, a one-dimensional model predicts a negative exponential probability distribution with $P(W_S|W_p) \approx \langle \widehat{W}_S \rangle^{-1} \exp(-W_S/\langle \widehat{W}_S \rangle)$ [30].

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

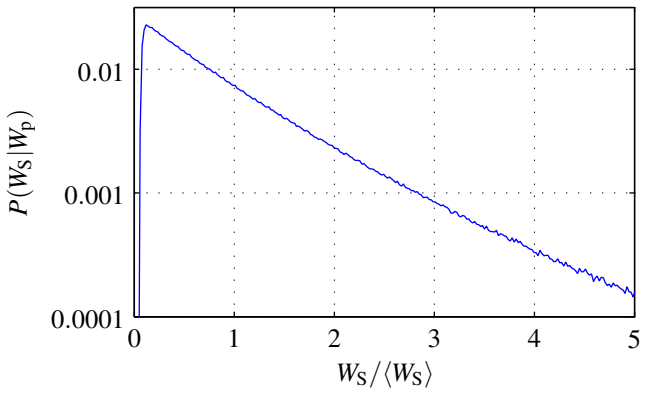

Fig. 3. Plot of the measured Stokes pulse energy distribution $P(W_S|W_p)$ as a function of the normalized Stokes pulse energy $W_S/\langle W_S\rangle$ for a single pump pulse energy value $W_p = \langle W_p\rangle$.

In agreement with the one-dimensional model, the measured distribution shown in Fig. 3 is predominantly a negative exponential. The non-exponential behaviour in Fig. 3 at $W_S \approx 0$ occurs because the Stokes light is not perfectly single mode. The scattered Stokes light contains weak contributions from other spatio-temporal modes due to phonon decay and coupling of the pump to more than one spatial mode [34, 38]. In SISRS sources where many spatio-temporal modes are excited, the coherence of the output light decreases and the Stokes pulse energy fluctuations diminish [34]. However, in the case of Fig. 3, large energy fluctations are easily resolved, allowing us to convert the raw data to random bits.

4. Data processing

Bias and classical noise are inevitably mixed in with the quantum randomnesss we use to generate random bits. There are numerous approaches to remove bias and extract unbiased random bits from raw data. We use Toeplitz-hashing as a randomness extractor [23, 24]. The extractor is applied by multiplying concatenated binary strings of raw data, each of length s bits, with a $m \times s$ random seed Toeplitz matrix to output m random bits; the seed matrix can be used repeatedly because the hash function is a strong extractor [24]. The value of m is set by the quantum random information content of the data as we discuss below.

The amount of randomness in the Stokes energy W_S can be quantified by its min-entropy,

$$H_\infty(W_S) = -\log_2\left[\max_{w_S} P(W_S = w_S)\right],$$

where W_S takes the value w_S with probability $P(W_S = w_S)$. When implementing the randomness extractor, the min-entropy places a limit on the number of statistically uncorrelated random bits that can be extracted from the input bit string. Assuming that any classical sources of noise may be known to an adversary, classical side-information must be accounted for in our evaluation of the min-entropy in order to ensure the security of the randomness extraction. Pump pulse energy fluctuations and electrical detection noise are the two principal sources of classical noise present in our experiment. Firstly, we bin the measured Stokes energy according to the measured input pump pulse energy to isolate the effect of pump energy fluctuations changing the Raman gain. We then calculate the quantum random contribution to the min-entropy by deconvolving the Stokes energy distribution from the detector noise, measured in

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

the absence of a signal. This allows us to place a minimum bound on the quantum information content available for randomness extraction from the raw data. The min-entropy of each Stokes distribution conditional on the pump taking value w_{p} is,

$$\tilde{H}_{\infty}(W_{\mathrm{S}}|W_{\mathrm{p}}=w_{\mathrm{p}}) = -\log_2\left[\max_{w_{\mathrm{S}}}\tilde{P}(W_{\mathrm{S}}=w_{\mathrm{S}}|W_{\mathrm{p}}=w_{\mathrm{p}})\right], \tag{1}$$

where the tilde denotes that the noise distribution has been deconvolved. Evaluating (1) for the measured data we find that $\tilde{H}_{\infty}(W_{\mathrm{S}}|W_{\mathrm{p}}=w_{\mathrm{p}}) > 4.2$ bits for all w_{p}. Completing the same procedure without first deconvolving the noise changes the conditional min-entropy by less than 0.1 bits, verifying that the electrical detection noise is small compared to the SISRS signal. We concatenate blocks of 512×8 bit measurements into strings of length $s = 4096$ bits, each with min-entropy $k = 512\times\tilde{H}_{\infty}(W_{\mathrm{S}}|W_{\mathrm{p}}) = 2150$ bits. To produce output bits ε-close to an ideal random distribution, the first dimension of the Toeplitz matrix is given by $m = k + 2\log_2\varepsilon$ where ε is a security parameter [24]. We use a security parameter of $\varepsilon = 2^{-200}$ so that $m = 2150 - 400 = 1750$ bits; this yields a corresponding entropy extraction of 3.4 bits per measurement. We populate the leading row and column of the seed Toeplitz matrix using a binary sequence obtained from our Stokes phase noise QRNG [22].

We tested the statistical properties of our random binary strings using the Diehard test suite [39]. The Diehard tests run on 11 MB binary files, and each test returns a p-value on $[0,1)$. For a good source of random bits, the output p-values should be uniform on $[0,1)$; clear failure of a test is indicated by p-values close to 0 or 1, up to several significant figures. The generally-accepted significance level α for "passing" a test is $0.01 < \alpha < 0.99$ [16]. As is shown in Table 1, the data passes all of the Diehard tests within this range. This confirms that

Table 1. Results of the Diehard statistical tests applied to the Raman random number bit strings. The p-values are within the significance interval $0.01 < \alpha < 0.99$, indicating that the bit strings pass all the tests.

Statistical Test	p-value[†]
Birthday spacings	0.697654 (KS)[‡]
Overlapping 5-permutation	0.975194
Binary rank test for 31×31 matrices	0.855622
Binary rank test for 32×32 matrices	0.366405
Binary rank test for 6×8 matrices	0.738437 (KS)
Bitstream	0.97565
OPSO	0.9776
OQSO	0.0733
DNA	0.9613
Count the 1's test	0.921504
Count the 1's test for specific bytes	0.980469
Parking lot	(KS) 0.765380
Minimum distance	0.358708 (KS)
3D Spheres	0.173700 (KS)
Squeeze	0.766849
Overlapping sums	0.487934 (KS)
Runs	0.944194 (KS)
Craps	0.154073

[†] For tests with multiple p-values the worst case was selected.
[‡] KS indicates a Kolmogorov-Smirnov test.

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013

Stokes pulse energy fluctuations are an effective source of statistically uncorrelated, unbiased bit-strings.

5. Conclusion

We have introduced and demonstrated a technique for generating sequences of quantum random bits by measuring the randomly fluctuating pulse energies of Stokes pulses generated via SISRS. The randomness of the bits is guaranteed by the quantum mechanical origin of the Stokes pulse energy fluctuations. The energy fluctuations are visible to the naked eye, and are easily measured using high speed PIN photodiodes. Since the pulse energy is a continuous variable, multiple random bits can be extracted from each measurement by digitizing the output from a detector with sufficiently high resolution. After Stokes generation, optical phonons typically decay on picosecond timescales so the vacuum state is quickly reset; new, statistically independent Stokes pulses can therefore be generated in rapid succession.

Diamond was used as the scattering substrate due to its high Raman gain and broad transparency. Its large Stokes shift, and that of other similar Raman active media [40], permit the use of ultrafast picosecond and femtosecond pump pulses. Diamond's rapid phonon decay means that GHz, or higher, pulse repetition rates are possible. However, the propagation length in bulk diamond is limited by diffraction of the pump beam, which in turn limits the SISRS gain available for a given pump pulse energy. The current implementation was therefore limited to 1 kHz by the need to boost the pump pulse energy using a laser amplifier. Increases to the SISRS gain above our operating value by further increasing the pump pulse energy were limited by the onset of optical damage to the substrate. As a result, the SISRS gain was unsaturated, restricting the width of the Stokes pulse energy distribution and, therefore, the number of bits extracted to 3.4 bits per measurement. A higher bit extraction per measurement could be obtained by partially saturating the SISRS gain to give a more favourable Stokes pulse energy distribution which is less biased toward $W_S = 0$. For example, a longer interaction region and therefore higher SISRS gain could be achieved by placing the substrate in a cavity, or by use of an integrated photonic structure such as a gas-filled photonic crystal fiber [41]. We expect that a longer interaction region will also enable the use of low power laser oscillators operating at GHz repetition rates, leading to commensurate high speed random bit production.

Acknowledgments

This work was supported in part by the Natural Sciences and Engineering Research Council of Canada. The authors wish to thank Serguei Patchkovskii for helpful discussions.

#197725 - $15.00 USD Received 16 Sep 2013; revised 1 Nov 2013; accepted 2 Nov 2013; published 20 Nov 2013