Quantum random bit generation using stimulated Raman scattering

Philip J. Bustard,[1,2] Doug Moffatt,[2] Rune Lausten,[2] Guorong Wu,[2] Ian A. Walmsley,[1] and Benjamin J. Sussman[2,*]

[1]*Clarendon Laboratory, University of Oxford, Parks Road, Oxford, OX1 3PU, UK*
[2]*Steacie Institute for Molecular Sciences, National Research Council of Canada, 100 Sussex Drive, Ottawa, Ontario, K1A 0R6, Canada*

[*]*ben.sussman@nrc.ca*

Abstract: Random number sequences are a critical resource in a wide variety of information systems, including applications in cryptography, simulation, and data sampling. We introduce a quantum random number generator based on the phase measurement of Stokes light generated by amplification of zero-point vacuum fluctuations using stimulated Raman scattering. This is an example of quantum noise amplification using the most noise-free process possible: near unitary quantum evolution. The use of phase offers robustness to classical pump noise and the ability to generate multiple bits per measurement. The Stokes light is generated with high intensity and as a result, fast detectors with high signal-to-noise ratios can be used for measurement, eliminating the need for single-photon sensitive devices. The demonstrated implementation uses optical phonons in bulk diamond.

OCIS codes: (190.5650) Raman effect; (190.5890) Scattering, stimulated; (290.5910) Scattering, stimulated Raman; (270.2500) Fluctuations, relaxations, and noise; (350.5030) Phase; (030.6600) Statistical optics.

References and links

1. G. Marsaglia, "On the randomness of pi and other decimal expansions," InterStat **5** (2005).
2. 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).
3. H. Schmidt, "Quantum mechanical random number generator," J. Appl. Phys. **41**, 462–468 (1970).
4. 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).
5. 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).
6. W. Wei and H. Guo, "Bias-free true random-number generator," Opt. Lett. **34**, 1876–1878 (2009).
7. 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).
8. 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).
9. 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).
10. 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).
11. U. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory **39**, 733 –742 (1993).
12. A. Penzkofer, A. Laubereau, and W. Kaiser, "High intensity Raman interactions," Prog. Quantum Electron. **6**, 55 (1979).
13. M. G. Raymer and I. A. Walmsley, "Quantum coherence properties of stimulated Raman scattering," Prog. Opt. **28**, 181 (1990).

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

14. M. G. Raymer, K. Rzążewski, and J. Mostowski, "Pulse-energy statistics in stimulated Raman scattering," Opt. Lett. **7**, 71–73 (1982).
15. I. A. Walmsley and M. G. Raymer, "Observation of macroscopic quantum fluctuations in stimulated Raman scattering," Phys. Rev. Lett. **50**, 962–965 (1983).
16. 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).
17. 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).
18. 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 (1993).
19. 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.
20. 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," Diam. Relat. Mater. **19**, 1289 – 1295 (2010).
21. M. G. Raymer and J. Mostowski, "Stimulated Raman scattering: unified treatment of spontaneous initiation and spatial propagation," Phys. Rev. A **24**, 1980–1993 (1981).
22. J. von Neumann, "Various techniques used in connection with random digits," Nat. Bur. Stand., Appl. Math Ser. **12**, 36–38 (1951).
23. A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer, "How to turn loaded dice into fair coins," IEEE Trans. Inf. Theory **46**, 911 –921 (2000).
24. C. Gerry and P. Knight, *Introductory Quantum Optics* (Cambridge Univ Pr, 2005).
25. G. Marsaglia, "Diehard battery of tests of randomness," http://www.stat.fsu.edu/pub/diehard/.
26. H. Haken, *Encyclopedia of Physics*, vol. 25 (Springer, 1970).
27. W. Louisell, *Quantum Statistical Properties of Radiation* (John Wiley and Sons, Inc., New York, 1973).

1. Introduction

Random number sequences are an essential component of modern information networks. They are used as keys for secure communications, as orderings for random sampling in simulations and data analysis, and are an important part of trustworthy gaming and lotteries. Traditional methods for generating random numbers rely on deterministic algorithms or deterministic physical processes. For example, the digits of π can be used as random numbers [1], but they are deterministically calculable and hence unsuitable for a cryptographic key: if an adversary determines the sequence used, the process is compromised. Therefore deterministic generation systems are unsuitable for high security applications.

Quantum mechanical systems are the the only known entities that exhibit non-deterministic behaviour. While the evolution of a quantum mechanical wavefunction is deterministic, the outcome of a particular measurement on a state is not, unless the system is already in an eigenstate of the chosen observable. Measurement of a suitable quantum observable can therefore provide non-deterministic outcomes which may be used as a source of true random numbers. In recent years quantum random number generators (QRNGs) have been designed using a variety of quantum effects including: vacuum shot noise [2], radioactive decay [3], laser noise [4, 5], photon statistics in weak coherent states [6–9], and fluorescence from entangled ions [10].

As data network speeds increase, so too does the need for high-speed QRNGs. Furthermore, certain security protocols require extremely long sequences [11]. Here we consider a QRNG with the potential for Tbps (10^{12} bits per second) bit-rates based on phase measurement of Raman scattered light in the macroscopic regime. In a typical Raman scattering process, an input pump photon is annihilated on scattering from a vibrational excitation, and a longer wavelength Stokes photon is created, with the residual energy deposited in the medium as a vibrational quantum, or phonon. The stimulated scattering of pump photons into the Stokes field can be described classically, however the spontaneous initiation of Raman scattering in a Raman generator in the absence of an input Stokes field, or phonons, is a purely quantum phenomenon [12]. In a single-pass Raman generator, Stokes photons scattered from the pump field via an induced virtual level stimulate further emissions, resulting in a macroscopic Stokes

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

field. The spontaneous emission to the Stokes field is due to the quantum mechanical zero-point motion of the phonon field [13]. Under suitable conditions, the quantum statistics of the spontaneous noise responsible for the Stokes field can be preserved and amplified to a macroscopic level. Here we use the most noise-free amplification process possible: the near unitary evolution of an almost pure vacuum state into a state with highly unpredictable values of its physical observables. This unpredictability may be observed either in photon number (Stokes pulse energy) [14, 15], or in the optical phase [16–18]. The quantum uncertainty in these measurable parameters is therefore suitable as a source for QRNG. Phase and energy measurements of a macroscopic Stokes field may be executed with high precision using high-bandwidth, sensitive photodetectors, such as PIN diodes. This enables detection with simple and robust technology. Higher precision measurements have higher bit-depths and therefore multiple random bits can be extracted from a single measurement. In the case of Stokes photon number, a stable pump pulse source is required to avoid masking the quantum statistics with pump pulse energy fluctuations [15]; this stringent requirement is not necessary for observation of the Stokes phase fluctuations. In our experiment we used the optical phase measurement of Stokes light output by transient stimulated Raman scattering from a Raman generator. The demonstrated Raman phase technique has the potential to generate very high bit-rates and rapid turn-on times because the non-resonant nature of the Raman interaction allows broad-bandwidth, ultrashort pulses to be used and because rapid system dephasing promptly resets the vacuum state before each phase is generated. Dephasing times of 1-10 ps are found in bulk solids, in liquids, and even in some gases [19]; the physical limit to data rates is then in excess of 1 Tbps. While this is beyond the rate demonstrated here, significant improvements toward this limit can be envisaged with the use of high gain waveguides and fast detection.

2. Experiment

We use diamond as the active medium in our Raman generator, shown in Fig. 1. As an optical material, diamond is unparalleled in its high Raman gain and wide transparency range, permitting a compact and reliable design. 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 with frequency $\Omega = 1332\,\mathrm{cm}^{-1}$. At room temperature the Boltzmann population ratio between the optical phonon band $|2\rangle$ and the acoustic phonon band $|1\rangle$ is 1.7×10^{-3}, and therefore thermal excitation is negligible. A linearly-polarized pump pulse with duration $\tau_p = 100\,\mathrm{ps}$, energy $\mathscr{E}_p$=1.6 μJ, and wavelength $\lambda_p = 532\,\mathrm{nm}$, is focussed into a 3 mm CVD diamond plate oriented along the $\langle 100\rangle$ axis. The pump generates longitudinal optical phonons at Ω, and a Stokes pulse with mean energy 0.16 μJ is emitted at $\lambda_S = 573\,\mathrm{nm}$; this gives a photon conversion efficiency to the Stokes field of $\eta = 0.11$. The dephasing time for the vibrational excitation is estimated at $\Gamma^{-1} = 7\,\mathrm{ps}$, based on the Raman linewidth and transient coherent ultrafast phonon spectroscopy measurements [20], yielding $\Gamma\tau_p = 14$. Using η and an analytic result for the Stokes pulse energy taken from the fully quantum model [21], we estimate the Raman gain to be $gL \approx 29$, where g is the steady-state Raman gain coefficient and L is the gain length of the diamond. The experimental parameters therefore satisfy the necessary conditions for transient SRS ($gL > \Gamma\tau_p$) in the high-gain limit ($gL\Gamma\tau_p \gg 1$) [13]. The emitted Stokes light therefore has a smooth temporal profile with a well-defined, but random, phase.

A reference pulse is generated using the same pump pulse in an identical setup to the signal pulse; this is allowed because each Stokes field has no phase-correlation with the pump field [18]. However, in principle, the reference field does not have to be generated by stimulated Raman scattering since it is only used to make a relative measurement of the signal Stokes's random phase. The Stokes pulse and the reference pulse are combined at a beamsplitter. A small lateral tilt Δk is introduced and the resulting fringe pattern is recorded on a 2048-pixel

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

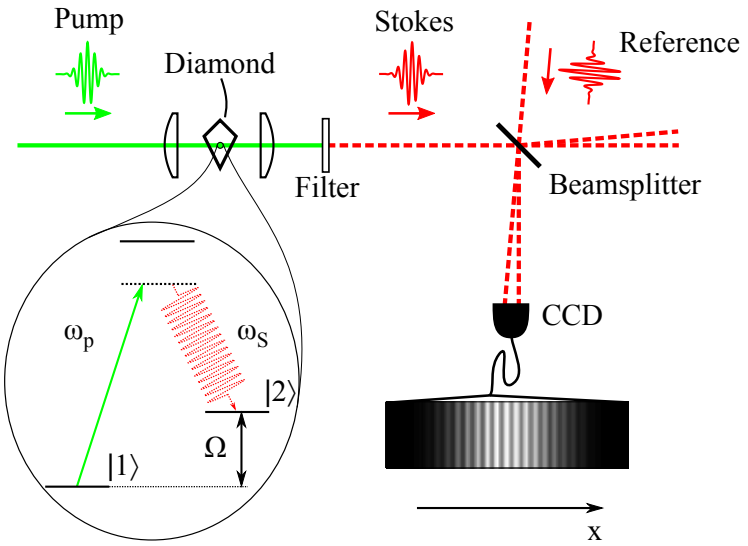

Fig. 1. Schematic diagram of Raman random number generator. A pump pulse is focussed into a 3 mm CVD diamond plate, generating a Stokes field with random phase. The pump field is filtered out using a bandpass filter, leaving only the Stokes field which is then combined with a reference pulse at a beamsplitter. A small lateral tilt is introduced and an interferogram is then measured using a linear CCD array. Inset: A Λ-level diagram shows the Raman transition in diamond used to generate the randomly-phased Raman Stokes light. Pump photons at 532 nm are annihilated; Stokes photons at 573 nm are generated along with vibrational phonons at $\Omega = 1332\,\mathrm{cm}^{-1}$.

line array charge-coupled device (CCD) camera operating at 200 Hz. The fringe measurement is a comparison of the first Stokes field $|A_S|e^{-i(\Delta kx+\phi_S)}$ with the reference Stokes field $|A_r|e^{-i\phi_r}$, where $A_{S,r}$ are the field amplitudes, Δk is the difference in wavevectors in the plane of the detector, x is the position coordinate along the camera array, and $\phi_{r,S}$ are the field phases. This yields an interferogram given by $S_{int} \propto |A_S||A_r|\cos(\Delta kx+\Delta\phi)$ where $\Delta\phi = (\phi_S - \phi_r)$ is a phase factor lying randomly on the interval $0 \leq \Delta\phi < 2\pi$ due to the quantum mechanical origin of ϕ_S.

Acquisition rates are currently hardware limited by CCD readout and pump laser repetition (1 kHz). The switch to a high-rate detection scheme (*e.g.*, heterodyne) and high-repetition, or CW, lasers could significantly improve on these practical limitations. Phase-correlations between Stokes fields from serial pump pulses can persist for many dephasing times, with the correlations expected to expire when the coherent excitation level falls below the zero-point quantum level of one phonon per mode [17, 18]. The ultimate physical limit on measurement rates is therefore dictated by the requirement that coherent phonons remaining in the diamond from a Stokes pulse generation event should decay below the quantum level of one phonon per mode before a subsequent pump pulse arrives. We can estimate this limit by equating the number of phonons with the number of Stokes photons emitted, assuming that all of the phonons generated are in a single mode. The number of coherent optical phonons is expected to decay as $e^{-2\Gamma\tau}$, where τ is the delay [18]. Here, for the average Stokes pulse photon number of 4.6×10^{11}, this gives an average of 0.1 phonons remaining after a delay of 102 ps. The physical limit to measurement rates in diamond is then 9.8 GHz, although higher rates should be possible in Raman media with shorter dephasing times.

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

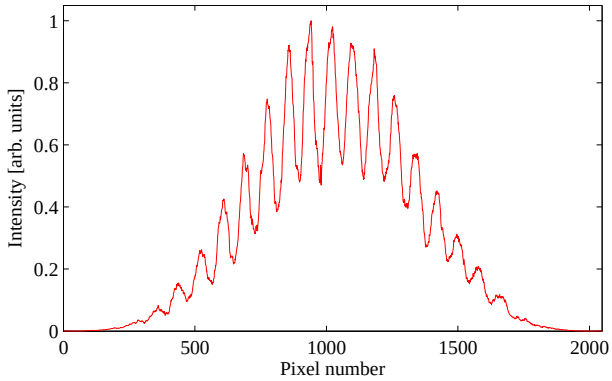

Fig. 2. Typical interferogram of two Stokes pulses generated by spontaneously initiated stimulated Raman scattering. The fringe phase is random for each measurement.

3. Results

Figure 2 shows a typical interferogram. As the process relies on the large amplification of vacuum fluctuations, the measurement is in the macroscopic limit of a quantum phenomenon. The interferograms are used to generate random bits by fitting to a cosine and extracting the phase. A higher precision measurement produces a larger number of bits. The phase measurement may therefore produce multiple bits per shot; here we generate 6 bits per measurement (distinguishing $2^6 = 64$ possible phases). Any possible bias in the phase measurement is removed by post-processing using a fair bit extractor algorithm [22, 23]. The ultimate limit for bit generation per shot is set by the minimum phase defined $\Delta\phi_{min}$. When the Raman process is strong, the coherence of the Stokes light approaches that of the pump, a coherent state, and therefore the minimum phase defined depends on the number of photons per pulse n as approximately $\Delta\phi_{min} \sim 1/n$ [24].

We tested the randomness of the Raman phase measurements using the standard DIEHARD statistical test suite [25]. As is shown in Table 1, the data set passed all the tests, confirming that the measured optical phase is a suitable source of random numbers.

4. Theoretical framework

To understand the origins of the phase fluctuations used in Raman random number generation, we refer to the one-dimensional quantum mechanical equations of motion for SRS [13, 21]. We consider the coupled equations for the Stokes field operator $\hat{E}_S^{(-)}(z,\tau)$ and the collective vibrational phonon lowering operator $\hat{Q}^\dagger(z,\tau)$ for the ensemble of two-level vibrational systems with lower energy state $|1\rangle$ and upper energy state $|2\rangle$; z is the propagation coordinate and $\tau = t - z/c$ is the time in the pulse frame. Assuming that the population inversion of the vibrational levels is negligibly modified by the SRS, and that the pump pulse E_p is not depleted during the propagation such that $E_p = E_p(\tau)$, the coupled equations take the linearized form,

$$\partial_z \hat{E}_S^{(-)}(z,\tau) = -i\kappa_2 E_p(\tau)\hat{Q}^\dagger(z,\tau) \quad (1)$$

$$\partial_\tau \hat{Q}^\dagger(z,\tau) = -\Gamma\hat{Q}^\dagger(z,\tau) + \hat{F}^\dagger(z,\tau) + i\kappa_1 E_p^*(\tau)\hat{E}_S^{(-)}(z,\tau). \quad (2)$$

Equation (1) describes the growth of the Stokes field with propagation distance, while Eq. (2) governs the evolution of the vibrational lowering operator $\hat{Q}^\dagger(z,\tau)$; κ_1 and κ_2 are related to the steady-state Raman gain coefficient g by $g = 2\kappa_1\kappa_2|E_p|^2/\Gamma$ and $\kappa_2 = 2\pi N h \kappa_1^*/\lambda_S$ where

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

Table 1. Results of the DIEHARD statistical tests imposed on the Raman random number bit strings.

Statistical Test	p-value[†]	Result
Birthday spacings	0.140289 (KS)[‡]	Success
Overlapping 5-permutation	0.234407	Success
Binary rank test for 31×31 matrices	0.857819	Success
Binary rank test for 32×32 matrices	0.888548	Success
Binary rank test for 6×8 matrices	0.595644 (KS)	Success
Bitstream	0.11249	Success
OPSO	0.0547	Success
OQSO	0.0806	Success
DNA	0.0247	Success
Count the 1's test	0.217644	Success
Count the 1's test for specific bytes	0.171729	Success
Parking lot	0.437972 (KS)	Success
Minimum distance	0.312133 (KS)	Success
3D Spheres	0.012979 (KS)	Success
Squeeze	0.344869	Success
Overlapping sums	0.100233 (KS)	Success
Runs	0.101465 (KS)	Success
Craps	0.213158	Success

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

c is the speed of light in vacuo, E_p is the pump field amplitude, h is Planck's constant, and N is the number of scattering atoms per unit volume. The phonon mode will eventually decay due to coupling with other degrees of freedom not included in the model. In diamond, the mechanism is principally due to anharmonic decay and lattice impurities. This is accounted for phenomenologically by adding two terms on the right hand side of Eq. (2) following the results of quantum reservoir theory [26, 27]. The first term accounts for damping of the vibrational excitation at rate Γ, while the second term $\hat{F}^\dagger(z,\tau)$ is a Langevin operator which maintains the expectation values of the commutation relations for the $\hat{Q}(z,\tau)$ operator [13]. The Langevin operator and vibrational phonon operator have the following properties,

$$\langle \hat{Q}^\dagger(z,0)\hat{Q}(z',0)\rangle = \frac{1}{\rho}\delta(z-z'), \tag{3}$$

$$\langle \hat{F}^\dagger(z,\tau)\rangle = \langle \hat{F}(z,\tau)\rangle = 0, \tag{4a}$$

$$\langle \hat{F}^\dagger(z,\tau)\hat{F}(z',\tau')\rangle = \frac{2\Gamma}{\rho}\delta(z-z')\delta(\tau-\tau'), \tag{4b}$$

$$\langle \hat{F}(z,\tau)\hat{F}^\dagger(z',\tau')\rangle = 0, \tag{4c}$$

where ρ is the number of molecules per unit length. The noise introduced by the Langevin operator is delta-correlated, meaning that it is completely random from moment to moment; this property determines the statistics of the Stokes field, as will be seen below. In the absence of a pump field, the solution to Eq. (2) is,

$$\hat{Q}^\dagger(z,\tau) = \int_{-\infty}^{\tau} \hat{F}^\dagger(z,\tau')e^{-\Gamma(\tau-\tau')}\mathrm{d}\tau'. \tag{5}$$

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

This expresses the fact that zero-point noise in the phonon field is intimately related to the white noise introduced from the quantum reservoir via the Langevin operator [13].

Solving by Laplace transform, with the assumption of no input field $\hat{E}_S^{(-)}(0,\tau)|\Psi(0)\rangle = 0$ and no initial excitation $\langle \hat{Q}(z,0)\hat{Q}^\dagger(z,0)\rangle = 0$, the Stokes field initiated by spontaneous Raman scattering is given by [21],

$$\hat{E}_S^{(-)}(L,\tau) = -i\kappa_2 E_p(\tau)\int_{-\infty}^{\tau} \mathrm{d}\tau' \int_0^L \mathrm{d}z \left[e^{-\Gamma(\tau-\tau')}K(L,z;\tau,\tau')\hat{F}^\dagger(z,\tau')\right], \tag{6}$$

where

$$K(L,z;\tau,\tau') = I_0(\sqrt{4\kappa_1\kappa_2(L-z)p(\tau,\tau')}),$$

and

$$p(\tau_1,\tau_2) = \int_{\tau_2}^{\tau_1} \mathrm{d}\tau\, |E_p(\tau)|^2.$$

To prove the suitability of the Stokes light as a source of random phase, we consider an interferometric measurement of the Stokes field compared to an arbitrary reference field E_r at a small lateral tilt Δk. In the plane of the detector these fields are given by $\hat{E}_S = \hat{E}_S^{(-)}(L,\tau)e^{i(\omega_S\tau-\Delta kx)}$ and $E_r = |E_r(z,\tau)|e^{i(\omega_S\tau+\phi_r)}$, where ϕ_r is arbitrary. The oscillating part of the interferogram is then given by,

$$S_{int} \propto |E_r(z,\tau)|\hat{E}_S^{(-)}(L,\tau)e^{-i(\Delta kx+\phi_r)} + \text{h.c.} \tag{7}$$

Taking the expectation value of Eq. (7),

$$\langle S_{int}\rangle = G_1\left[\langle F^\dagger(z,\tau')\rangle\right] + G_2[\langle F(z,\tau')\rangle\big] = 0, \tag{8}$$

where Eq. (4a) and Eq. (6) were used, and $G_i[\langle f(z,\tau)\rangle]$ denotes a functional of $f(z,\tau)$. The Stokes field initiated from spontaneous Raman scattering is therefore not phase correlated with any reference phase ϕ_r, and is inherently random. An interferometric measurement of the Stokes field optical phase relative to any suitable reference will then yield a random number between 0 and 2π on any given measurement.

5. Conclusion

We have introduced a technique for generating random bits by measuring the phase of light generated by stimulated Raman amplification of vacuum fluctuations. The Raman amplification raises the intensity of the fluctuations to levels that are easily measured with macroscopic optical techniques. Rapid dephasing of typical optical phonons (picoseconds) permits new, statistically independent, phases to be generated in rapid succession. As the transient Stokes light phase is determined only by the vacuum field, the technique is insensitive to pump pulse energy fluctuations, avoiding the possibility of classical fluctuations masquerading as quantum fluctuations. The phase may be measured to high precision, affording the possibility of generating multiple bits per measurement.

The Raman active material used here was diamond owing to its high Raman gain and broad transparency. Its large Stokes shift, and that of some other Raman active media, raises the possibility of using ultrafast pump pulses, permitting a turn-on time of femtoseconds. The current hardware implementation is limited to 1 kHz. However, the ultimate physical rate is set by the product of the measurement rate and the bit-depth per measurement. The measurement rate is limited by the phonon reset time, as discussed above. Diamond has the longest phonon decay time of any solid; in comparison, $LiNbO_3$, for example, decays ten times faster and still has high Raman gain [19]. This suggests that measurement rates of 100 GHz are feasible without

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011

compromising randomness. In this demonstration 6 bits were extracted per measurement, although much higher bit-depths should be possible, in principle. Therefore the product of the measurement rate and the bit-depth per measurement could exceed 1 Tbps. Importantly, this would be realizable with fast, high signal-to-noise ratio photodetectors, thus eliminating the need to work with challenging single-photon sensitive devices.

#155284 - $15.00 USD Received 26 Sep 2011; revised 7 Oct 2011; accepted 21 Oct 2011; published 23 Nov 2011