Quantum Random Bit Generation using Energy Fluctuations in stimulated Raman Scattering

Prepared by:

Philip J. Bustard, Duncan G. England, Josh Nunn, Doug Moffatt,
Michael Spanner, Rune Lausten, Benjamin J. Sussman

National Research Council
1200 Montreal Road
Ottawa, Ontario K1A 0R6

March 31 2013

CSA:

Benjamin J. Sussman

March 2017

DRDC-RDDC-2017-C050

This page intentionally left blank.

Quantum random bit generation using energy fluctuations in stimulated Raman scattering

Philip J. Bustard, Duncan G. England, Josh Nunn, Doug Moffatt,
Michael Spanner, Rune Lausten and Benjamin J. Sussman

31 March 2013

1 Introduction

Random binary keys (RBKs) are a critical resource in modern cyber security systems. They are used to convert plain text messages into secure ciphers for transmission over open channels. The rapid growth in the scale and speed of digital networks has resulted in an increased need for high quality RBKs in high volume to facilitate secure information transfer in applications where privacy is paramount. RBK generation methods based on classical processes or computer algorithms may be compromised if an adversary determines the algorithm used and then predicts the value of future keys. Quantum random bit generators (QRBGs) can create keys with guaranteed security because they use fundamentally random outcomes from measurements on suitable quantum systems. Here we summarize our QRBG research results; we measured pulse energy fluctuations in Stokes light from spontaneously initiated stimulated Raman scattering (SISRS) and converted the measurements to truly random, unbiased binary sequences. The principal results of our research are summarized as follows:

1. SISRS can be used to amplify broadband vacuum fluctuations of the electromagnetic field to levels which are easily measured using fast, inexpensive photodiodes.
2. Random fluctuations can be measured in the pulse energy of Stokes pulses generated using SISRS.
3. Measured Stokes pulse energies can be converted to high-quality RBKs which pass standard tests of randomness.

2 Spontaneously initiated stimulated Raman scattering

Raman scattering is the inelastic scattering of photons from vibrational, rotational, or electronic excitations in the Raman-active medium. In our prototype QRBG 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

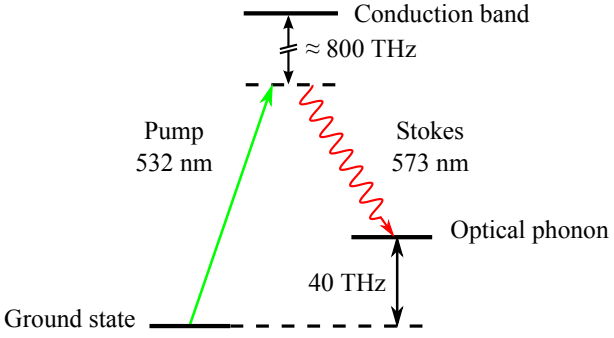

Figure 1: Λ-level diagram for Stokes Raman scattering in diamond. Inelastic scattering annihilates the pump photon at 532 nm, creating an optical phonon in the diamond and a red-shifted Stokes photon at 573 nm.

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 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 [1, 2]. The quantum mechanical origin of the Stokes pulse is, therefore, manifest in its pulse energy statistics [3, 4], making pulse energy measurements suitable for use in a QRBG.

3 Choice of substrate for SISRS

When selecting a SISRS substrate for use in our QRBG, we identified several key criteria to be assessed. Desirable properties for these criteria are summarized below:

Raman gain coefficient
A high Raman gain coefficient is desirable because it lowers the necessary pump pulse energy for efficient Stokes generation by SISRS.

Interaction length
Stokes conversion efficiency grows with the interaction length so that a long interaction region is desirable.

Optical geometry
A single pass optical geometry is simple to implement and the SISRS physics is well-understood.

Raman shift
A large Raman shift (*i.*) gives low thermal noise so that quantum noise dominates the Stokes emission and (*ii.*) means that the Stokes pulse can easily be spectrally filtered from the pump pulse.

Phonon decay
Rapid phonon decay means that the vacuum state of the substrate is quickly reset so that statistically independent Stokes pulses can be generated rapidly, thereby enhancing the RBK generation rate.

According to these criteria, we selected diamond for construction of a prototype device. Diamond has a high Raman gain, a large Raman shift, and a short phonon decay time of 3.5 ps, making it an excellent material for QRBG. Bulk diamond was easily interfaced with pump pulses from our available laser amplifier to produce Stokes pulses in a single pass geometry, making it a good choice for prototype QRBG development. However, one negative factor with any bulk substrate is that the interaction region is limited by beam spreading of the focussed pump pulse as it propagates. Beam spreading must therefore be mitigated by the use of intense pump pulses. Waveguiding can provide tight optical confinement of a pump pulse over a long interaction length, thereby enabling the use of low power pump pulses. We note that the construction of optical waveguides in diamond is an active area of research [5], so that the use of diamond waveguides may be possible in future.

Alternative Raman active waveguiding substrates may also provide positive options for future development. An ideal substrate will be one that can deliver high Raman gain with low power, ultrashort (fs or few-ps duration) pump pulses from a high repetition rate source. We have isolated several attractive options for future investigation. Their properties are qualitatively summarized in Table 1, relative to those of bulk diamond; options requiring future assessment in the laboratory are labelled with a "?".

	SISRS efficiency	Ultrashort compatible?	Raman shift	Decay rate
Bulk diamond	Moderate	100-ps pulses	Large	High
Gas-filled HCPCF[†] [6]	High	?	Large	Moderate
P_2O_5-doped fiber [7]	High	?	Moderate	High
KTP waveguide[‡] [8]	High	few-ps pulses	Moderate	High

[†] HCPCF: hollow-core photonic crystal fiber
[‡] KTP: Potassium titanyl phosphate

Table 1: Table qualitatively summarizing key attributes of potential Raman active substrates for SISRS.

Recently, we observed Stokes pulses generated by SISRS in a 3 cm KTP waveguide using low power, few-ps pulses from a laser oscillator. This advance will allow the future development of a MHz repetition rate prototype QRNG based on energy fluctuations from SISRS.

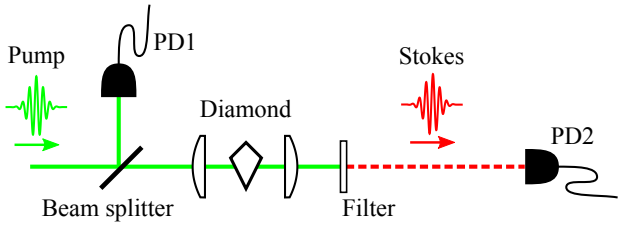

Figure 2: Experimental setup: the pump pulse is focussed into a diamond plate, generating a Stokes sideband by SISRS. The Stokes pulse is spectrally-filtered from the pump, and its energy is measured by photodiode PD2. Part of the pump pulse energy is separated using a beamsplitter in front of the diamond,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

4 Prototype QRBG device

Diamond is used as the scattering medium in our prototype QRBG 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. At room temperature (T=300 K), thermal excitation of the optical phonon modes is negligible, with a Boltzmann ratio of $\exp(-\hbar\Omega/k_B T) = 1.7\times10^{-3}$ between the optical phonon band and the ground state. The dephasing time of the optical phonons is $\Gamma^{-1} = 7\,\mathrm{ps}$, based on the Raman linewidth and transient coherent ultrafast phonon spectroscopy measurements [9, 10]. 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 [11].

A linearly polarized pump laser operating at 1 kHz, with pulse duration $\tau_p = 100\,\mathrm{ps}$, mean pulse energy $W_p \simeq 1\,\mu\mathrm{J}$, and wavelength $\lambda_p = 532\,\mathrm{nm}$ is focussed 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 $\lambda_S = 573\,\mathrm{nm}$. Crucially, 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 the dynamics are coherent and dominated by a single temporal mode [4]. The spatial coherence of the Stokes beam is high because the pump is tightly focussed to a near diffraction-limited spot, with confocal parameter $b \approx 200\,\mu\mathrm{m}$ much shorter than the diamond sample; in this geometry the pump beam effectively acts as a spatial filter for the Stokes light [4]. After generation in the diamond crystal, the Stokes pulse is collimated and spectrally filtered from the pump. The Stokes beam is focussed on to a fast photodiode (PD2), whose response is electronically integrated and recorded as a measure of the Stokes pulse energy W_S. As a reference, we also measure the pump pulse energy W_p on each shot using a fast photodiode (PD1) in front of the diamond.

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 record a reference measurement of the pump pulse energy W_p in front of the diamond using photodiode PD1. 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 conditional 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 [12].

5 Theoretical background

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 ge-

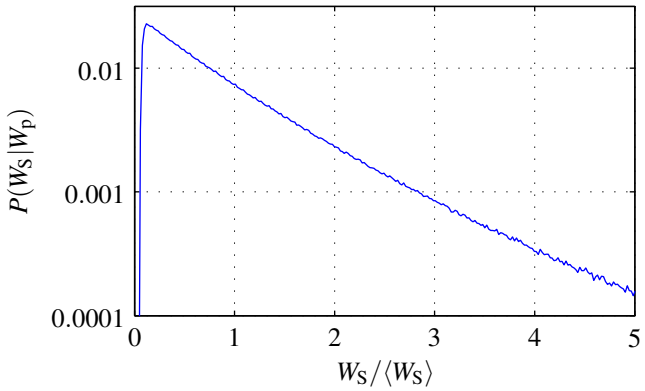

Figure 3: Plot of the measured Stokes pulse energy distribution $P(W_S|W_p)$ as a function of the normalized Stokes pulse energy $W_S/\langle W_S\rangle$ for a single pump pulse energy value $W_p = \langle W_p\rangle$.

ometry, and the influence of phonon decay on the scattering process [4]. 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 $P(W_S|W_p) \approx \langle\widehat{W}_S\rangle^{-1}\exp(-W_S/\langle\widehat{W}_S\rangle)$ [3].

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 [4, 13]. In SISRS sources where many spatio-temporal modes are excited, the coherence of the output light diminishes and the Stokes pulse energy fluctuations diminish [4]. However, in the case of Fig. 3, large energy fluctations are easily resolved, allowing us to convert the raw data to random bits.

6 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 a Toeplitz-hashing randomness extractor [14, 15].

The min-entropy [16] of the raw data 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 noise must be excluded from our calculation of the min-entropy in order to ensure the security of the randomness extractor. Pump pulse energy fluctuations and electrical detection noise are the two principal sources of classical noise present in our experiment. We bin the Stokes energy measurements according to the measured input pump pulse energies W_p to isolate the effect of pump energy fluctuations changing the Raman gain. We subsequently deconvolve the Stokes energy distribution from the measured detection noise distribution. The min-entropy per Stokes energy measurement is given by $H_\infty(W_S|W_p) = -\log_2\left[\max\tilde{P}(W_S|W_p)\right]$, where $\left[\max\tilde{P}(W_S|W_p)\right]$ is the probability of the most frequent outcome after binning on the pump energy and deconvolving the noise distribution. Deconvolving the noise reduces the min-entropy by less than 0.1 bits for all pump pulse energies, and is therefore a small effect. The min-entropy per measurement is $H_\infty > 4.2$ bits for all values of the pump energy. Using a security parameter of 2^{-200} in the Toeplitz randomness extractor [15], we extract 3.4 bits per measurement.

We tested the statistical properties of our random binary strings using the DIEHARD test suite [17]. 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. In the literature, the generally-accepted significance level α for "passing" a test is $0.01 < \alpha < 0.99$ [18]. As is shown in Table 2, the data passes all of the DIEHARD tests within this range. This confirms that measuring Stokes pulse energy fluctuations is an effective way to generate statistically uncorrelated, unbiased bit-strings.

Statistical Test	p-value[†]	Result
Birthday spacings	0.697654 (KS)[‡]	Pass
Overlapping 5-permutation	0.975194	Pass
Binary rank test for 31×31 matrices	0.855622	Pass
Binary rank test for 32×32 matrices	0.366405	Pass
Binary rank test for 6×8 matrices	0.738437 (KS)	Pass
Bitstream	.97565	Pass
OPSO	0.9776	Pass
OQSO	0.0733	Pass
DNA	0.9613	Pass
Count the 1's test	0.921504	Pass
Count the 1's test for specific bytes	0.980469	Pass
Parking lot	(KS) 0.765380	Pass
Minimum distance	0.358708 (KS)	Pass
3D Spheres	0.173700 (KS)	Pass
Squeeze	0.766849	Pass
Overlapping sums	0.487934 (KS)	Pass
Runs	0.944194 (KS)	Pass
Craps	0.154073	Pass

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

Table 2: 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.

7 Discussion

Our QRBG 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 dephasing 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 non-quantum noise in the pump laser and detection system. Combining the potential repetition rate and the potential bit extraction depth, the estimated physical limit to data rates is in excess of 1 terabit per second.

8 Conclusion

We have introduced and demonstrated a technique for generating sequences of quantum random bits by measuring the randomly fluctuating pulse energy of Stokes light 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 photodiodes. Since the pulse energy is a continuous variable, multiple random bits can be extracted from a single measurement. 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 [19], permit the use of ultrafast picosecond and femtosecond pump pulses. Diamond's rapid phonon decay means that GHz pulse repetition rates are possible. However, the propagation length in bulk diamond is limited by spreading 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. Use of cavities or integrated photonic structures such as gas-filled photonic crystal fibers [6] will increase the SISRS gain and allow the use of laser oscillators with GHz repetition rates, leading to commensurate high speed random bit production.

References

[1] A. Penzkofer, A. Laubereau, and W. Kaiser, "High intensity Raman interactions," Prog. in Quantum Electronics **6**, 55 (1979).

[2] M. G. Raymer and J. Mostowski, "Stimulated Raman scattering: Unified treatment of spontaneous initiation and spatial propagation," Phys. Rev. A **24**, 1980–1993 (1981).

[3] M. G. Raymer, K. Rzążewski, and J. Mostowski, "Pulse-energy statistics in stimulated Raman scattering," Opt. Lett. **7**, 71–73 (1982).

[4] 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).

[5] M. P. Hiscocks, K. Ganesan, B. C. Gibson, S. T. Huntington, F. Ladouceur, and S. Prawer, "Diamond waveguides fabricated by reactive ion etching," Opt. Express **16**, 19,512–19,519 (2008).

[6] 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 (2002).

[7] W. A. Gambling, D. Payne, C. Hammond, and S. Norman, "Special issue paper. optical fibres based on phosphosilicate glass," Electrical Engineers, Proceedings of the Institution of **123**, 570–576 (1976).

[8] F. Laurell, J. B. Brown, and J. D. Bierlein, "Sum-frequency generation in segmented ktp waveguides," Applied Physics Letters **60**, 1064–1066 (1992).

[9] 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**, 155,201 (2008).

[10] 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).

[11] 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," Nature Photon. **6**, 41 (2011).

[12] 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).

[13] 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).

[14] 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 Berlin Heidelberg, 1994), pp. 129–139.

[15] 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**, 062,327 (2013).

[16] S. Barnett, *Quantum information*, vol. 16 (Oxford University Press, 2009).

[17] G. Marsaglia, "Diehard battery of tests of randomness," www.stat.fsu.edu/pub/diehard/ (1995).

[18] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," App. Phys. Lett. **93**, 031109 (2008).

[19] J. Reintjes and M. Bashkansky, *Handbook of Optics, Volume IV: Optical Properties of Materials, Nonlinear Optics, Quantum Optics* (McGraw-Hill Professional, 2010), chap. 15, p. 15.1, 3rd ed.