Quantum random number generator based on spin noise

G. E. Katsoprinakis, M. Polis, A. Tavernarakis, A. T. Dellis, and I. K. Kominis*
Department of Physics, University of Crete, Heraklion 71103, Greece
and Institute of Electronic Structure and Laser, Foundation for Research and Technology, Heraklion 71110, Greece
(Received 6 November 2007; published 19 May 2008)

We present an implementation of a robust quantum random number generator based on the quantum fluctuations of the collective spin of an alkali-metal vapor. The achieved bit rate is limited by the spin relaxation rate of the alkali-metal atoms $1/T_2$ to about 1 kbit/s. However, the same physical scheme, which is impervious to limitations posed by single-photon detectors used in current implementations and rests solely on threshold detection, can be extended to solid state systems with a bit rate higher than 1 Gbit/s.

DOI: 10.1103/PhysRevA.77.054101 PACS number(s): 03.65.Ta

I. INTRODUCTION

Random numbers are indispensable for a wide range of applications, from numerical simulations of complex physical systems [1] to testing Bell's inequalities [2]. Recently, with the advent of quantum information science, and in particular, with the development of quantum communication and quantum cryptography protocols [3,4], random numbers satisfying particular criteria are necessary. The basic requirement is obviously related to the degree of "randomness" of the generated series of bits. It has been shown [5] that Monte Carlo simulations using pseudorandom numbers generated algorithmically can produce erroneous results. Physical random number generators (RNGs) have thus emerged as reliable sources of randomness, the latter relying on the practically unpredictable behavior of a complex or chaotic system. However, were adequate computational power available, the prediction of the evolution of a classical system would be fundamentally possible. Quantum random number generators (QRNGs), on the other hand, take advantage of the inherent randomness of quantum systems, thus providing a series of random bits which is by no means predictable. Radioactive sources have been used as QRNGs [6], but so far the most versatile generators rely on a quantum dilemma of single photons [7,8], i.e., the "which-way" decision a photon has to make when crossing a beam splitter, with each of the two possible outcomes corresponding to the bits "0" and "1."

In this work we report on a QRNG which is limited by the autocorrelation time of the quantum system, works with a coherent light beam and hence is not limited by the autocorrelation time of single-photon detectors. The physical system used for the random bit generation is an alkali-metal vapor. The randomness stems from the quantum fluctuations of the collective atomic spin, known as spin noise, which is of its own interest due to the connection with precision measurements [9]. The achievable random bit rate of this generator is limited by the transverse spin relaxation rate of the alkali-metal vapor $1/T_2$, since T_2 determines the correlation time of the quantum noise signal used to generate the random bits. If not the only one, this is one among the very few cases where a high relaxation rate is desirable. This is analogous to the desire for a short coherence time of the photon source in the optical random number generators [7]. The presented spin noise QRNG is much slower than the optical generators, however, a similar scheme using solid state systems [10,11] has the potential to provide for random bit rates higher by several orders of magnitude. In the following we will describe the experimental apparatus and the method of the random bit sequence generation. We will then focus on answering the two prevalent questions regarding every QRNG: (a) is it quantum and (b) is it random.

II. GENERATION OF RANDOM BITS FROM SPIN NOISE

The experimental setup shown in Fig. 1 will be briefly described as it is similar to the one used in Ref. [12]. A diode laser provides a probe beam up to a power of 30 mW, and is blue-detuned by 30 GHz from the rubidium $D1$ line. The laser is linearly polarized before entering the rubidium cell. The spontaneous spin noise of the rubidium vapor induces noise in the paramagnetic Faraday rotation angle of the probe laser, which is measured with a balanced polarimeter. The noise spectrum is centered at the Larmor frequency $\omega_L = 28$ kHz due to the presence of a transverse magnetic field $B_z = 60$ mG. The polarimeter signal is band-pass filtered, amplified and registered at a personal computer with a DAQ card. The data processing and the random bit generation are performed by LabView®. A typical spin noise signal is shown in Fig. 2(a). The sequence of random bits is obtained as follows: with the magnetic field turned off we monitor the level of background noise thus defining a positive (and a negative) threshold. With the magnetic field turned on, the

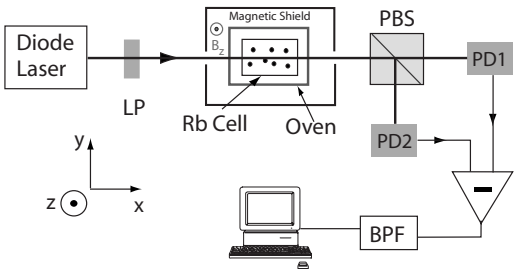

FIG. 1. Experimental setup. LP, linear polarizer; PBS, polarizing beam splitter; PD, photodiode; BPF, band-pass filter.

*ikominis@iesl.forth.gr

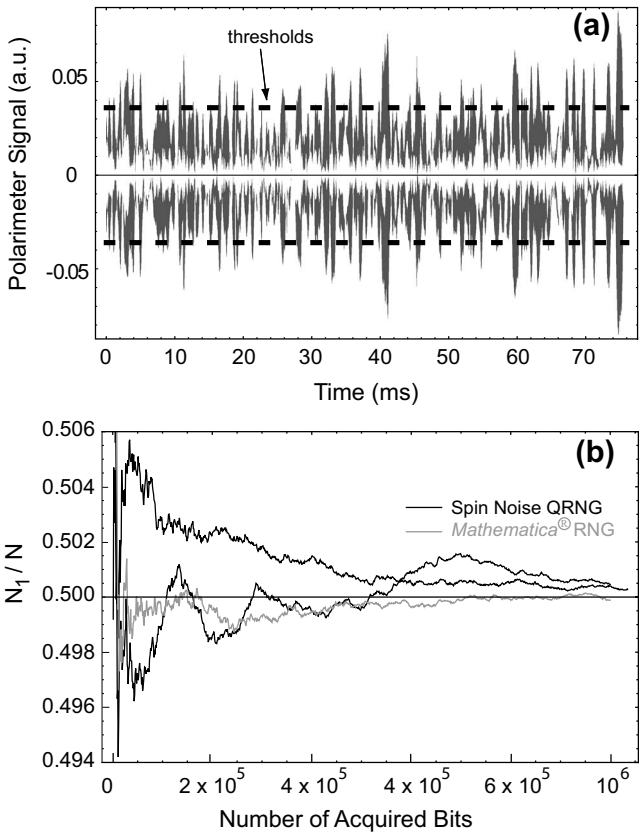

FIG. 2. (a) Polarimeter signal as a function of time. Filter output noise without spins (magnetic field off) is shown in white, spin noise signal (magnetic field on) is shown in gray. The dashed lines are the positive and negative thresholds, which when exceeded, produce the random bits "1" and "0," respectively. (b) Evolution of the ratio N_1/N with the number of acquired bits. We show two different realizations of the spin noise QRNG, each consisting of 10^6 bits, along with one produced with the RNG of MATHEMATICA®. N_1 is the number of 1's among the N bits.

bit "1" ("0") is registered when the spin noise signal exceeds the positive (negative) threshold. That this is a random event can be first seen with a basic randomness test, namely, the ratio of "1's" (or "0's") to the total number of acquired bits. As expected and shown in Fig. 2(b) this ratio tends to 1/2 for large enough number of acquired bits. More elaborate randomness tests will be presented in Sec. IV. Since spin noise is [12] an Ornstein-Uhlenbeck stochastic process, its autocorrelation is [15] $e^{-\tau/T_2}$, where $1/T_2$ is the half-width of the spin noise resonance (see inset of Fig. 3). In our operating conditions $1/T_2 \approx 10$ kHz, so that with the chosen threshold and the resulting bit rate of 1 kbit/s, the autocorrelation is e^{-10}, i.e., one out of 22 000 bits is correlated with its neighbor. This figure can obviously be increased at the expense of the bit rate by choosing a higher threshold. We have also verified that the distributions of both the noise (electronic + photon shot noise) and the signal (spin noise) amplitudes N and $S_{\rm sp}$, are Gaussian, with respective widths σ_n and $\sigma_{\rm sp} = 2\sigma_n$. The probability P for a wrong bit assignment is the probability that the polarimeter signal exceeds the positive (negative) threshold when the spin noise signal is negative (positive). If $p(S_{\rm sp},N)$ is the joint probability density and S_0 the threshold value, it is $P=\int_{-\infty}^{0} dS_{\rm sp} \int_{S_0-S_{\rm sp}}^{\infty} dN p(S_{\rm sp},N)$. For a threshold $S_0=5\sigma_n$ that we use, $P \approx 10^{-8}$, proving that this QRNG is highly robust.

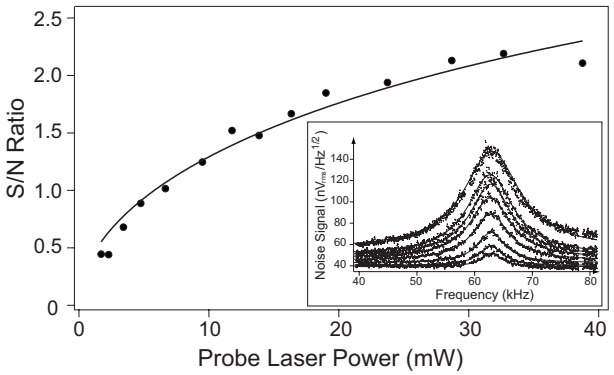

FIG. 3. Signal to noise ratio vs probe laser power, showing the saturating behavior expected from a spin noise signal. What is plotted is the square root of Eq. (1). Inset: part of the set of spin noise spectra used for the curve.

Furthermore, the magnetic resonance broadening is solely due to the irreversible dephasing of the spins brought about by atomic collisions and by light broadening [13]. Dephasing due to magnetic gradients, which in our case are less than 0.3 mG/cm, results [14] in a broadening of less than 20 Hz out of 10 kHz total width. Reversible spin relaxation which could lead to bit correlations is thus negligible. Since the atoms reside in a magnetic shield and have zero average spin polarization, there is no way that a coherent external manipulation can induce any correlations in the spin noise signal.

III. IS SPIN NOISE QUANTUM NOISE?

We will first show that the acquired signal is indeed a noise signal and not a coherent signal due to, e.g., optical pumping. This is usually proved [12] by the fact that the signal integrated power is proportional to the atom number $N_{\rm at}$. Here we use a new method, namely, the scaling of the signal-to-noise ratio with the probe beam power. If b is the broadening due to atomic collisions and transit time effects, then the spin noise power spectrum, centered at ω_L, will have a power-broadened half-width $1/T_2 = aI + b$, where a is a constant and I the incident probe laser intensity. The polarimeter signal is equal to $2\Phi_{\rm sn} I$, where $\Phi_{\rm sn} \sim \langle S_x \rangle$ is the Faraday rotation angle, proportional to the expectation value of the ensemble spin projection along the laser propagation axis. Spin noise fluctuations of $\langle S_x \rangle$, and hence $\Phi_{\rm sn}$, are independent of laser power. Thus the power spectral density has a peak height S proportional to $\Phi_{\rm sn}^2 I^2/(aI+b)$. The background N, dominated by photon shot-noise, will be proportional to I, therefore

$$\frac{S}{N} \sim \frac{I}{aI+b}. \tag{1}$$

Thus the ratio S/N saturates at high intensities, as shown in Fig. 3. On the contrary, in the hypothetical presence of a nonzero circular polarization of the probe laser, the angle $\Phi_{\rm sn}$

would be proportional to I, and the ratio S/N would not saturate. We now turn to the question of whether spin noise is quantum noise. This is directly related to sensitive atomic magnetometers employing spin-polarized alkali-metal vapors [16], where spin noise fundamentally limits the achievable sensitivity. An unpolarized ensemble of N_{at} spin-1/2 atoms is described by the maximally mixed density matrix $\rho=1/2$. The ensemble uncertainty of the total spin S_x is $\Delta S_x = \sqrt{N_{\mathrm{at}}/4}$. This would produce a coherent signal $\langle S_x\rangle \sim \Delta S_x$ at the Larmor frequency ω_L were it not for the atomic collisions, which relax any nonzero value of $\langle S_x\rangle$ while at the same time driving fluctuations of $\langle S_x\rangle$ around the mean value of zero. Indeed, if we consider two atoms colliding along a given collision trajectory being initially in the translational angular momentum state $|m\rangle$ (the $\hat{\mathbf{z}}$ axis of the magnetic field is the quantization axis) and their spin state being described by the mixed state $\rho_s=1/4$, the total state will be $\rho=\rho_s \otimes |m\rangle\langle m|$. This will evolve after the action of the spin-spin interaction Hamiltonian [17] $\mathcal{H}_s$ to a new state $\rho' \approx \rho_s \otimes |m\rangle\langle m| + \Sigma_{j=0,\pm 1} c_j \rho'_{s,j} \otimes |m+j\rangle\langle m+j|$. Tracing out the unobserved translational degrees of freedom, which play the analogous role of the environment q-bits in the quantum trajectories description of relevant phenomena [18], leads to a change of the spin density matrix $\delta\rho_s = \Sigma_{j=0,\pm 1} c_j \rho'_{s,j}$. The $j=0$ term is responsible for fluctuations, whereas the $j=\pm 1$ terms cause dissipation. Thus spin noise is caused by the quantum mechanical uncertainty of the spin degrees of freedom combined with measurement-induced noise, where measurement in this case is due to the atomic collisions. Hence spin noise is quantum noise, i.e., it fully bears a fundamental unpredictability.

IV. TESTING RANDOMNESS

The sequences of random bits produced by our setup were put through a large number of tests, most of which are defined in [19]. In all cases sets of 10^5 to 10^6 bits were tested. Although such a number of bits is relatively small for some tests, no discrepancies from a truly random behavior were observed. For completeness, the results of some illustrative tests are presented. In Fig. 4(a) the number of occurrences of n-bit length blocks of consecutive zeros and ones is shown. As expected from a random sequence, both scale as 2^{-n} with almost equal proportionality factors. In Fig. 4(b) the bit-autocorrelation Γ_n between bits at distance n is depicted. As defined in Ref. [8],

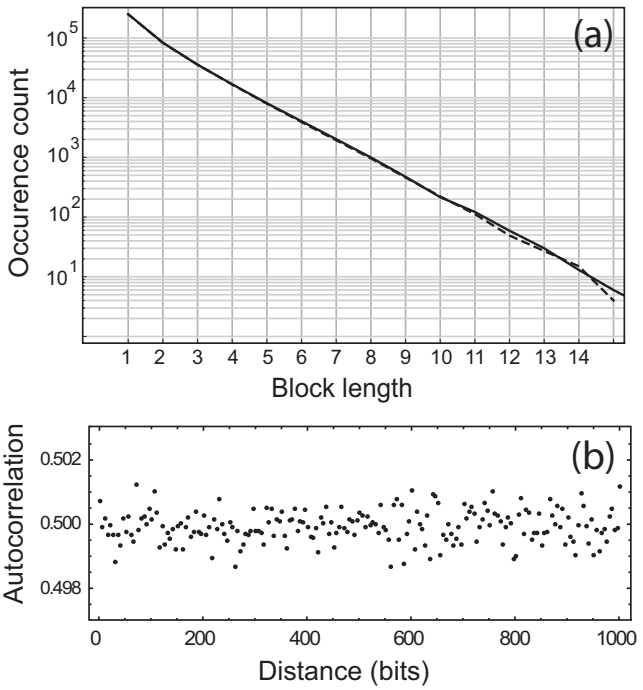

FIG. 4. (a) Occurrence of blocks of zeros (solid line) and ones (dashed line). (b) Bit autocorrelation as a function of bit distance n.

$$\Gamma_n = \frac{1}{N}\sum_{i=1}^{N-1} x_i \oplus x_{(i+n) \bmod N}. \tag{2}$$

For uncorrelated binary random variables A and B, $\mathrm{Var}(A \oplus B)=\frac{1}{4}$. Using the well-known statistical relations $\mathrm{Var}(X+Y)=\mathrm{Var}(X)+\mathrm{Var}(Y)$ and $\mathrm{Var}(aX+b)=a^2\mathrm{Var}(X)$ leads to $\mathrm{Var}(\Gamma_n)=\frac{1}{4N}$, which predicts a variance of 2.5×10^{-7} for our sample size, close to the measured value $\sim 2.9\times 10^{-7}$.

V. CONCLUSIONS

We have demonstrated a method for robust generation of a random bit sequence based on the quantum fluctuations of the collective spin of an alkali-metal vapor. This method only requires fast threshold detection and does not rely on efficient single photon detectors. To increase the bit rate, the same scheme could be applied to solid state systems. For example, conduction band spin fluctuations of donor electrons in bulk GaAs [10], with a spin noise resonance width on the order of 10 MHz, can lead to bit rates on the order of 10 Mbit/s or higher, depending on donor concentration. Similarly, in thin GaAs quantum well structures [11], the relevant dephasing rates are higher than 1 GHz, potentially leading to equally fast random bit rates.

[1] K. Binder, Rep. Prog. Phys. **60**, 487 (1997).
[2] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).
[3] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, and A. Zeilinger, Rev. Mod. Phys. **74**, 145 (2002).
[4] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[5] A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, Phys. Rev. Lett. **69**, 3382 (1992).
[6] H. Inoue, H. Kumahora, Y. Yoshizawa, M. Ichimura, and O.

Miyatake, Appl. Stat. **32**, 115 (1983).
[7] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).
[8] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 595 (2000).
[9] J. M. Geremia, J. K. Stockton, and H. Mabuchi, Phys. Rev. Lett. **94**, 203002 (2005).
[10] M. Oestreich, M. Römer, R. J. Haug, and D. Hägele, Phys. Rev. Lett. **95**, 216603 (2005).
[11] D. Stich *et al.*, Phys. Rev. Lett. **98**, 176401 (2007).
[12] G. E. Katsoprinakis, A. T. Dellis, and I. K. Kominis, Phys. Rev. A **75**, 042502 (2007).
[13] For the physical system we are using, i.e., in the absence of reversible dephasing, $T_2 \approx T_1$. A similar scheme with a system having a short T_1 could be also used, however, it would be vulnerable to low-frequency noise. In our case this is avoided with the application of the magnetic field that shifts the spin noise spectrum to a high frequency and automatically introduces the transverse coherence and the associated nomenclature of the transverse relaxation rate $1/T_2$, which as mentioned above, is indistinguishable from the population relaxation rate $1/T_1$.
[14] B. Julsgaard, J. Sherson, J. L. Sørensen, and E. S. Polzik, J. Opt. B: Quantum Semiclassical Opt. **6**, 5 (2004).
[15] D. T. Gillespie, Am. J. Phys. **64**, 225 (1996).
[16] D. Budker and M. V. Romalis, Nat. Phys. **3**, 227 (2007).
[17] S. Appelt *et al.*, Phys. Rev. A **58**, 1412 (1998).
[18] T. A. Brun, Am. J. Phys. **70**, 719 (2002).
[19] A. Rukhin *et al.*, NIST Special Publication Report No. 800–22, 2001 (unpublished).