Random Number Generation by Brillouin-enhanced Four-wave-mixing in Polarization Maintaining Fiber

Pedro Tovar, Xiaoyi Bao

Department of Physics, University of Ottawa, 25 Templeton Street, Ottawa, Ontario K1N 6N5, Canada

ptovarbr@uottawa.ca, xiaoyi.bao@uottawa.ca

Abstract: We report a novel real-time true random number generator based on Brillouin-enhanced FWM. Random bit sequences produced from the idler's intensity fluctuation, due to position and time dependent stochastic birefringence changes, passed all NIST tests. © 2022 The Author(s)

1. Introduction

Random numbers generation (RNG) is a task that attracts much interest due to its relevance in many areas, such as scientific simulations, lotteries, computer networks and mainly secure communications. With recent advances and availability of over-the-top computer technology, pseudo-random numbers generated from algorithms are no longer adequate for secure data encryption: hardware real-time random number generator is needed. True random numbers are usually generated from unpredictable physical processes, and many photonics techniques have been developed with this purpose [1]. Most works approaches the problem locally, such that random numbers are generated in a central office, but cannot be used for secret-key distribution as an eavesdropper could intermediate the secret-key transmission and decrypt confidential messages. A few works have explored optical systems for both RNG and secret-key distribution [2, 3], but there is a trade-off between the randomness of generated keys and the correlation between shared keys, making the distribution of highly-correlated random keys a challenge. In this work we describe a new method for RNG based on Brillouin-enhanced four-wave-mixing (FWM) that has the potential to improve the correlation between shared keys while not compromising the keys' randomness.

2. Principle

Stimulated Brillouin scattering (SBS) in optical fibers is a process that can be defined either by classical wave theory or through quantum mechanics. Classically, a pump wave and a Stokes wave interact non-linearly coupled by an acoustic wave, which is thermally excited and initiated through electrostriction. The propagating acoustic wave modulates the fiber's refractive index, inducing a Brillouin dynamic grating (BDG) [4] scattering light through Bragg diffraction. The BDG backscatters the input light at a frequency down-shifted by $\nu_B(z) = 2n(z)V_a/\lambda$ due to the Doppler effect, where $n(z)$ is the position-dependent refractive index, V_a the acoustic velocity, and λ the wavelength. From a quantum mechanics perspective, a pump photon is annihilated while a Stokes photon and an acoustic phonon are created, conserving energy in the process. The acoustic phonon lifetime, with typical durations of 10 ns, adds an uncertainty to the shift frequency $\nu_B(z)$.

If polarization maintaining fibers (PMF) are considered, then each polarization axis will exhibit a different $\nu_B(z)$ due to the fiber's high-birefringence: $\Delta n(z) = n_x(z) - n_y(z)$. However, since the BDG is polarization independent, the same frequency shift is obtained at λ_x and λ_y provided that $2n_xV_a/\lambda_x = 2n_yV_a/\lambda_y$ [4]. By launching a pump laser at frequency $\nu_1(t) = c/\lambda_x(t)$ in the x-polarized axis and a probe laser at frequency $\nu_2(t) = c/\lambda_y(t)$ in the y-polarized axis, then four optical waves are involved in the process: (1) the pump wave; (2) the Stokes wave from pump light diffraction ($\nu_{1S}(z,t) = \nu_1(t) - \nu_B(z)$); (3) the probe wave; and (4) the Stokes wave from probe light diffraction ($\nu_{2S}(z,t) = \nu_2(t) - \nu_B(z)$). These four optical waves were shown to be an FWM process [5], where the idler wave ($\nu_{2S}(z,t)$) is only generated if the phase-matching condition (PMC) is satisfied:

$$\nu_{2S}(z,t)\hat{x} = \nu_2(t)\hat{x} - \nu_1(t)\hat{y} + \nu_{1S}(z,t)\hat{y} \tag{1}$$

Thus, the frequency difference between the pump and probe waves, $\Delta\nu = \nu_2 - \nu_1$, must be tuned to satisfy Eq. 1. It has been shown that $\Delta\nu$ is position and time-dependent and can be written in terms of the fiber birefringence as $\Delta\nu(z,t) = -\overline{\nu}\Delta n(z,t)/\overline{n}$ [6], where $\overline{\nu} = (\nu_2\hat{x} + \nu_1\hat{y})/2$ and $\overline{n} = (n_x + n_y)/2$. We rewrite the PMC as:

$$[\nu_2(t) - \nu_B(z)]\hat{x} - [\nu_1(t) - \nu_B(z)]\hat{y} + \frac{\overline{\nu}}{\overline{n}}\Delta n(z,t) = 0 \tag{2}$$

The equation above can be satisfied at a certain position $z = z_0$ and at a given time $t = t_0$. But the birefringence is known to be a non-stationary stochastic process that varies along the fiber causing random polarization mode dispersion (PMD). Even in PMFs, which have a high-birefringence introduced in the manufacturing process ($\sim 10^{-4}$), the instantaneous birefringence still fluctuates in a scale of the order of 10^{-6} [7], hence the birefringence is a position and time dependent parameter. In addition, the central frequencies of pump and probe lasers are also randomly changing due to both the natural laser linewidth and fluctuations of driving current and surrounding temperature, which also affect the PMC but in a smaller scale.

The average birefringence in long PMFs ($>$ hundreds of meters) was shown to vary by more than 10^{-5} along the fiber, or $\Delta\nu$ varying by more than $\sim$1 GHz [6]. Thus, by setting both pump and probe lasers to operate continuously (CW), and by tuning their frequency difference to be within the fiber's birefringence fluctuation range, then the instantaneous birefringence at every position of the fiber has the potential to satisfy Eq. 2. This means that even with high laser frequency fluctuation and randomly varying birefringence for every position, at some position (or even a few positions) the PMC will be satisfied. Still, the position at which the PMC is satisfied changes randomly and is unpredictable. Moreover, because the reflectivity of the BDG decays exponentially with position [6], small fluctuations in the parameters of Eq. 2 will cause a large intensity fluctuation of the idler signal. We make use of such fluctuations to generate random numbers, where the randomness source is threefold: uncertainty of $\nu_B(z)$ related to the acoustic phonon lifetime; birefringence fluctuation along the fiber; and pump/probe laser frequency fluctuation. Furthermore, since this RNG method consists of FWM, then for the creation of a idler photon a probe photon *must* be annihilated, given, ideally, a perfect -1 correlation between the transmitted and reflected probe waves, which is crucial for secret-key distribution. In this work we focus on the investigation of the randomness of the idler signal.

3. Experimental Results

Fig. 1(a) shows the experimental setup used for RNG. A DFB pump laser with 8 MHz-linewidth is amplified by an Erbium-doped fiber amplifier (EDFA) and launched in the slow axis of a 2 km-long PMF by means of a polarization beam splitter (PBS). A DFB probe laser with 10 MHz-linewidth is launched in the PMF through the same PBS but in the fast axis. The probe laser frequency ν_2 is tuned to be about 92.9 GHz higher than the pump laser frequency ν_1, as shown in Fig. 1(b). This value is consistent with [6], and it corresponds to the central $\Delta\nu$ at which it is possible to satisfy the PMC with a tolerance of $\pm$500 MHz. The reflected signal in the fast axis is captured by an optical circulator and amplified by an EDFA. The generated idler signal is filtered with an optical band-pass filter (OBPF) with 3 GHz-bandwidth and detected with an AC-coupled photodetector (PD). The detected signal is shown in Fig. 1(c), clearly indicating a strong fluctuation of the idler's intensity as expected, which is far above the PD noise level.

The distribution of intensities measured over 10 seconds is shown in Fig. 1(d). The resulting distribution could be fit with a Maxwell distribution, though with a small deviation from the fitting. The reason for a nearly Maxwell distribution depends on two factors. First, since the randomness source governing the idler's fluctuation is the fiber's birefringence, then the probability distribution should be closer to a Maxwellian; this is equivalent to random PMD-induced differential group delay, which depends on birefringence fluctuations and has a Maxwell distribution. Second, the lasers' frequency fluctuations and acoustic phonon lifetime also act as non-negligible random sources, contributing to the overall fluctuation of the idler's intensity and to a small deviation from the Maxwell distribution.

To further investigate the randomness of the detected signal we analyzed its autocorrelation trace, which is shown in Fig. 2(a). It is clear that spurious reflections at the fiber end – which were minimized by adding a small-radius loop in the output port of the PMF – have no impact to the idler's intensity fluctuation. Yet, for random bit generation, minimal post-processing techniques have to be employed to balance the intensity distribution over a threshold level before conversion to bits 0's and 1's. By adding a digital delay of 10 μs to one replica of the digitized

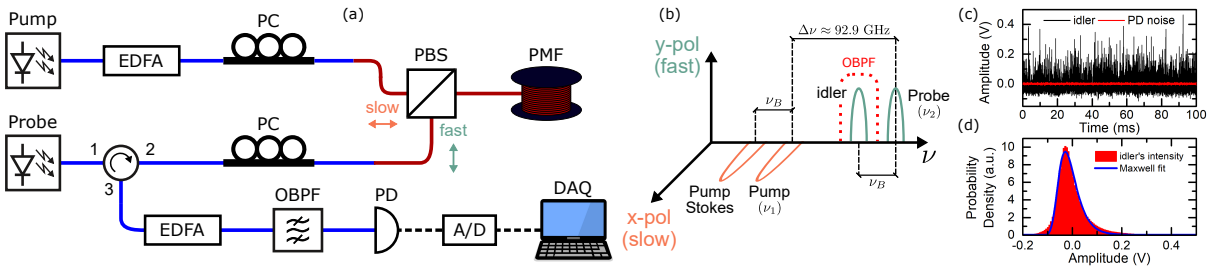

Fig. 1. (a) Experimental setup. (b) Illustration of optical spectral domain in the two orthogonal polarization axis in the PMF. (c) Intensity fluctuation of the idler signal, and (d) its intensity distribution.

detected signal (after analog-to-digital conversion, A/D) and subtracting the detected signal by its delayed-replica while sampling at a longer time of 20 μs to avoid negative correlation at the selected delay time, we generated the signal shown in Fig. 2(b). These operations could be done in the physical layer with the use of a beam-splitter, a fiber-spool delay and a balanced photodetector, thus not compromising the speed of the generated bit sequence. Moreover, this approach simplifies the selection of the threshold level to 0 V, and no arbitrary level had to be chosen or continuously-adjusted for every trace. The intensity distribution of the post-processed signal is shown in Fig. 2(c), exhibiting a third momentum equal to zero, being a balanced distribution and more suited for RNG.

Bit sequences were generated from measurements over 2 s, giving rise to sequences of 100 kbits. Fig. 2(d) shows an example of part of a bit sequence generated from the signal shown in Fig. 2(b), where bits were generated at a speed of 50 kbps. To visually inspect the randomness of generated bit sequences, we analyze the 2D bits map of the firsts 500×500 bits from generated sequences. An example is provided in Fig. 2(e), where no pattern is identified – blue pixels corresponding to 1's and red pixels to 0's. For a numerical analysis of the randomness, the bit sequences were submitted to the statistical tests defined by the National Institute of Standards and Technology (NIST). We tested 100 samples of 100 kbits with a significance value of 0.01, and the test results are listed in Table 1. To pass the tests, the uniformity o p-values must be greater than 0.0001, which is valid for all tests as can be seen in column 2 of Table 1. Also, it is required that the p-values obtained for all sequences are greater than the significance value in at least 96% of sequences for all tests. This condition is verified in column 3, proofing that the proposed method is valid for random number generation.

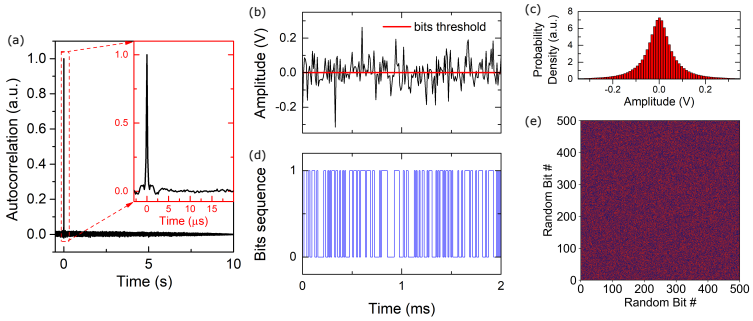

Table 1. NIST test results.

Statistical Test	*P*-Value	Proportion
Approximate Entropy	0.816537	97/100
Block Frequency	0.401199	99/100
Cumulative Sums	0.574903	99/100
FFT	0.554420	98/100
Frequency	0.779188	100/100
Linear Complexity	0.834308	100/100
Longest Run	0.122325	100/100
Non-Overlapping Template	0.003996	99/100
Overlapping Template	0.897763	100/100
Random Excursion	0.035174	97/100
Random Excursions Variant	0.008879	98/100
Rank	0.595549	98/100
Runs	0.935716	96/100
Serial	0.366918	97/100

Fig. 2. (a) Autocorrelation trace. (b) Post-processed signal with balanced fluctuations over 0 V. (c) Unskewed distribution of the post-processed signal. (d) Example of bit sequence generated. (e) 2D bit map from 500×500 bits – ones and zeros correspond to blue and red pixels, respectively.

4. Conclusions

A novel method for RNG was demonstrated based on Brillouin-enhanced FWM, where random bits were generated at a rate of 50 kbps, which could be improved with higher-speed instrumentation at the detection end and post-processing techniques. The generated bit sequences were submitted to the NIST suite of tests, passing in all statistical tests. Last, because the method involves FWM, the probe and idler waves are entangled, so that their intensities should be highly correlated, which is of great interest for secret-key distribution and is currently under experimental validation.

References

1. Joseph D. Hart et al. Recommendations and illustrations for the evaluation of photonic random number generators. *APL Photonics*, 2(9):090901, 2017.
2. Konstantin Kravtsov et al. Physical layer secret key generation for fiber-optical networks. *Opt. Express*, 21(20):23756–23771, Oct 2013.
3. Imam Uz Zaman et al. Physical Layer Cryptographic Key Generation by Exploiting PMD of an Optical Fiber Link. *Journal of Lightwave Technology*, 36(24):5903–5911, 2018.
4. Kwang Yong Song et al. All-optical dynamic grating generation based on Brillouin scattering in polarization-maintaining fiber. *Opt. Lett.*, 33(9):926–928, May 2008.
5. Da-Peng Zhou et al. Four-wave mixing analysis of Brillouin dynamic grating in a polarization-maintaining fiber: theory and experiment. *Opt. Express*, 19(21):20785–20798, Oct 2011.
6. Zichao Zhou et al. Dynamic detection of acoustic wave generated by polarization maintaining Brillouin random fiber laser. *APL Photonics*, 5(9):096101, 2020.
7. Yongkang Dong et al. Truly distributed birefringence measurement of polarization-maintaining fibers based on transient Brillouin grating. *Opt. Lett.*, 35(2):193–195, Jan 2010.