Fast and compact VCSEL-based quantum random number generator

Fast and compact VCSEL-based quantum random number generator

R Shakhovoy[1,2], E Maksimova[1,3*], V Sharoglazova[1,4], M Puplauskis[4,5], and Y Kurochkin[1,2,5,6]

[1]QRate, 100 Novaya str., Skolkovo, Russia
[2]NTI Center for Quantum Communications, National University of Science and Technology MISiS, 4 Leninsky prospekt, Moscow, Russia
[3]Peter the Great St. Petersburg Polytechnic University, 29 Polytechnicheskaya str., St. Petersburg, Russia
[4]Skolkovo Institute of Science and Technology, Bolshoy Boulevard 30, bld. 1, Moscow, Russia
[5]Russian Quantum Center, 45 Skolkovskoye Shosse, Moscow, Russia
[6]Moscow Institute of Physics and Technology, 9 Institutskiy per., Dolgoprudny, Russia

[*]e.maksimova@goqrate.com

Random number generators (RNGs) are an essential ingredient of modern cryptographic systems. Particular attention is paid today to a special class of RNGs – quantum RNGs, which are attracting close attention of researchers due to the explosive development of quantum key distribution systems, where the use of quantum randomness is a necessary security requirement. A large number of various quantum entropy sources have been proposed over the last 10-15 years. Most of them are based on the use of different quantum optics phenomena, particularly, on the effects occurring in semiconductor lasers. This choice is due to the relatively low cost and ease of use of such devices and the high random bit generation rate available with optical QRNGs. Motivated by these reasons, we study in the present research the QRNG based on variations of light polarization in a vertical-cavity surface-emitting laser (VCSEL). The scheme we propose allows creating an extremely compact and fast optical QRNG, consisting essentially of only a laser and a polarizing beam splitter. We revealed that it is possible to ensure the pulsed operation of a VCSEL in a bistable regime, which is characterized by random switch of light polarization. We show, however, that probabilistic properties of such laser pulses significantly depend on the internal laser parameters as well as on its operating mode. Understanding these properties is fundamentally important for the correct assessment of the quantum noise contribution and, consequently, for the subsequent post-processing of digitized random sequences.

Keywords: quantum random number generator, VCSEL

1. Introduction

Nowadays, vertical-cavity surface-emitting lasers (VSCELs) have one of the largest production volume among all types of semiconductor lasers and are of particular attention of scientific community, which is reflected by a huge number of publications on VCSELs [1]. Unlike edge-emitting lasers, the light output polarization in VCSELs is inherently unstable, inasmuch as there is no intrinsic and strong mechanism in VCSELs to select one specific orientation of the polarization. This feature is usually hampers the use of VCSELs in sensing and datacom applications, where stable

polarization is generally required; however, the effect of polarization switching may be useful in other applications, e.g., in random number generation. Indeed, at certain values of the pump current, VCSELs may operate in a bistable mode, where mode hopping occurs between the two linearly polarized states by the influence of spontaneous emission noise [1, 2]. It is well-known that spontaneous transitions are induced by zero-point oscillations of the electromagnetic field [3, 4], so spontaneous emission can be treated as amplified vacuum fluctuations and should be thus considered as quantum noise. Random polarization switching occurring in VSCELs may be, therefore, treated as a quantum entropy source.

Here, we propose a concept of a quantum random number generator (QRNG) based on variations of light polarization in VCSEL operating in a pulsed regime. The QRNG scheme comprises a VCSEL, a polarizing beam splitter (PBS) and a photodetector, which performs the polarization-resolved measurement of laser pulses. We demonstrate below that this scheme may be used to implement a fast and compact QRNG.

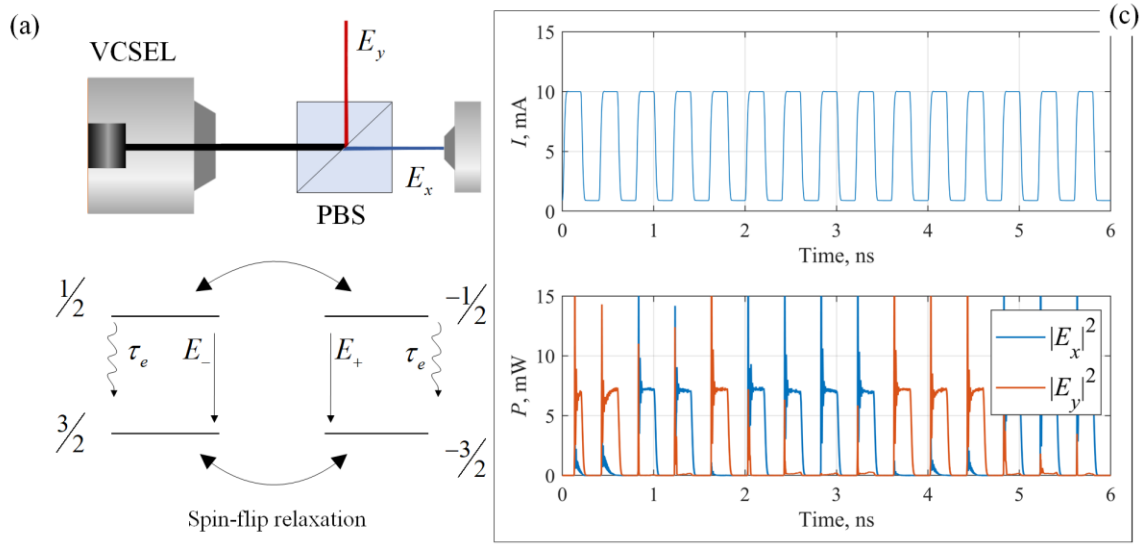

Figure 1. (a) The concept of a VCSEL-based QRNG. (b) The energy diagram corresponding to the spin-flip model. (c) Injection current pulses (above) and corresponding simulation of polarization-resolved pulse sequences at the VCSEL output (below).

2. Simulations

To describe the polarization dynamics in a VCSEL, we used the well-known spin-flip model (Fig. 1(b)) [5], which implies the existence of two spin subsystems related to the right and left circularly polarized light (the amplitudes of the corresponding fields are denoted in Fig. 1 by E_+ and E_-, respectively). The two subsystems are assumed to be coupled just via the spin-flip processes, i.e. their interaction Hamiltonian is zero. The model is also complemented by linear dichroism γ_a and birefringence γ_p [6] and is represented by the following system of rate equations written in terms of linearly polarized fields:

$$\begin{aligned}
\dot{E}_x &= \frac{1}{2\tau_{ph}}(1+i\alpha)\left[\left(G_L-1\right)E_x + i\mathcal{B}dE_y\right] - \left(\gamma_a + i\gamma_p\right)E_x + F_x,\\
\dot{E}_y &= \frac{1}{2\tau_{ph}}(1+i\alpha)\left[\left(G_L-1\right)E_y - i\mathcal{B}dE_x\right] + \left(\gamma_a + i\gamma_p\right)E_y + F_y,\\
\dot{N} &= \frac{I}{e} - \frac{N}{\tau_e} - \frac{1}{\tau_{ph}}G_L\left(\left|E_x\right|^2 + \left|E_y\right|^2\right) - i\frac{1}{\tau_{ph}}\mathcal{B}d\left(E_x^*E_y - E_y^*E_x\right),\\
\dot{d} &= -\frac{d}{\tau_d} - \frac{i}{\tau_{ph}}G_L\left(E_x^*E_y - E_y^*E_x\right) - \frac{1}{\tau_{ph}}\mathcal{B}d\left(\left|E_x\right|^2 + \left|E_y\right|^2\right),
\end{aligned} \tag{1}$$

where α is the linewidth enhancement factor (the Henry factor [7]) typically lying in the range 2-7, N is the total number of carriers (electrons), d is the difference between carrier inversions with opposite spins, $G_L = \left(N - N_{tr}\right)/\left(N_{th} - N_{tr}\right)$ is the normalized linear gain, $\mathcal{B} = 1/\left(N_{th} - N_{tr}\right)$ represents the slope of the gain, and Langevin forces F_x, F_y are given by

$$\begin{aligned}
F_x &= \sqrt{\frac{C_{sp}}{4\tau_e}}\left(\xi_+\sqrt{N+d} + \xi_-\sqrt{N-d}\right),\\
F_y &= -i\sqrt{\frac{C_{sp}}{4\tau_e}}\left(\xi_+\sqrt{N+d} - \xi_-\sqrt{N-d}\right).
\end{aligned} \tag{2}$$

The values of laser parameters used in simulations in Fig. 1(c) are: photon lifetime $\tau_{ph} = 1$ ps, electron lifetime $\tau_e = 1$ ns, spin-flip time $\tau_d = 1.25$ ps, linewidth enhancement factor $\alpha = 2$, transparency carrier number $N_{tr} = 5.94\times10^6$, threshold carrier number $N_{th} = 6.25\times10^6$, spontaneous emission coupling factor $C_{sp} = 10^{-4}$, linear dichroism $\gamma_a = -0.1$ GHz, linear birefringence $\gamma_p/2\pi = 28.65$ GHz.

For further simulations, we introduced the parameter R corresponding to the ratio between the intensity of the polarization mode and the total pulse intensity, which may be defined as $R = \max\left(R_x, R_y\right)$, where $R_x = \left|E_x\right|^2 \Big/ \left(\left|E_x\right|^2 + \left|E_y\right|^2\right)$ and $R_y = \left|E_y\right|^2 \Big/ \left(\left|E_x\right|^2 + \left|E_y\right|^2\right)$. In Fig. 2, we demonstrate the results of simulations for the dependence of R on different time parameters of the laser. (Other parameters were fixed and were taken as listed above.) Each point on the curves in Fig. 2 was calculated by averaging 10000 pulses similar to those shown in Fig. 1. Ideally, we would like to have $R \to 1$, i.e. we wish that for a particular pulse the whole intensity goes into a single polarization mode. However, one can see from Fig. 2 that the best value of R was found to be around 0.8, and this value occurs at very small values of the linewidth enhancement factor and the values of the spin-flip time close to the photon lifetime. At moderate values of α and τ_d, elliptical polarization generally occurs in a pulse. It is also interesting to note that R is almost independent on the photon lifetime at $\tau_{ph} > 1$ ps.

Another interesting feature to follow is the probability of occurrence of pulses with orthogonal polarizations. Here, we performed simulations at various sets of parameters and revealed that this probability is extremely sensitive to variations of laser time parameters and also on the values of γ_p and γ_a. In Fig. 3, we presented the result of simulations at parameters yielding equal probability of occurrence of pulses with orthogonal polarizations.

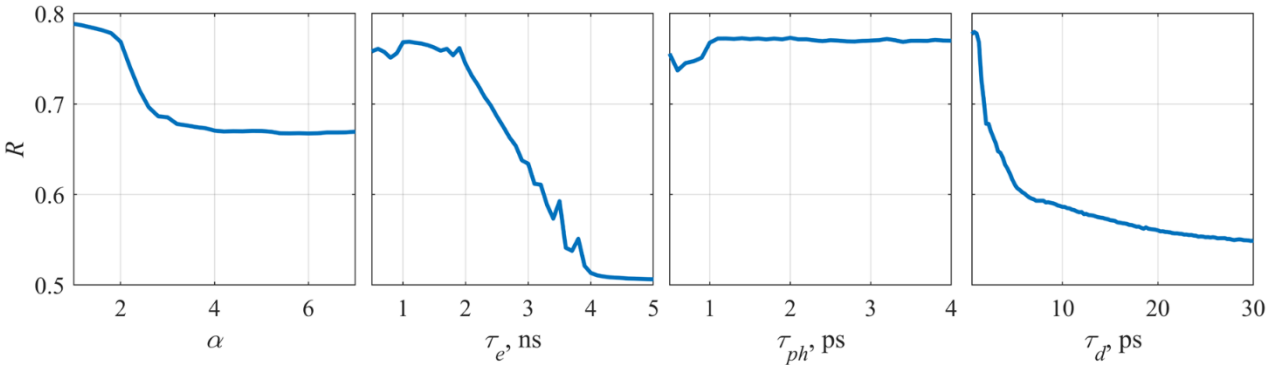

Figure 2. The dependence of *R* on (from left to right): the linewidth enhancement factor, the effective carrier lifetime, the photon lifetime, and the spin-flip time.

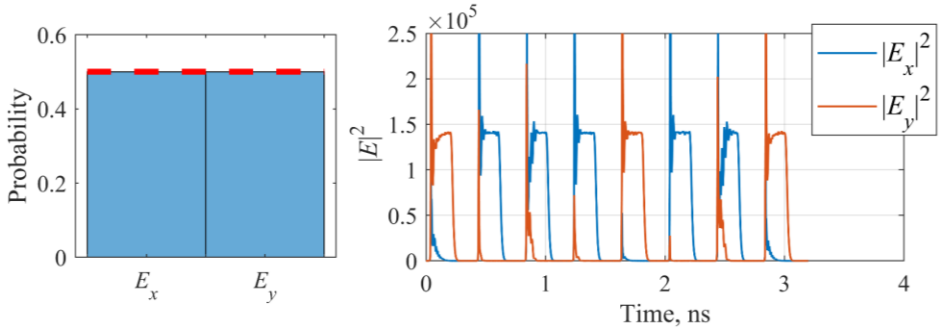

Figure 3. (Left) Probability of occurrence of pulses with orthogonal polarizations. Histograms were calculated from 10000 pulses with parameters $\tau_{ph} = 2.5$ ps, $\gamma_p/2\pi = 15.92$ GHz (other parameters were taken from Table 1). (Right) Example of a corresponding polarization-resolved pulse train.

3. Conclusion

We demonstrated that laser pulses from a gain-switched VCSEL operating in a polarization bistable mode could be used as a quantum entropy source. We revealed that it is difficult to achieve a mode of operation, when the whole intensity goes into a single polarization mode in various laser pulses; however, it is still possible to achieve equiprobable occurrence of pulses with (predominantly) orthogonal polarizations.

Acknowledgments

This work was supported by Russian Science Foundation (grant no. 17-71-20146).

[1] Michalzik R 2013 *VCSELs: Fundamentals, Technology and Applications of Vertical-Cavity Surface-Emitting Lasers* (Heidelberg: Springer-Verlag) pp 558
[2] Giacomelli G, Marin F, Gabrysch M, Gulden K H, and Moser M 1998 Polarization competition and noise properties of VCSELs *Optics Communications* **146** pp 136-140
[3] Loudon R 2000 *The Quantum Theory of Light* (Oxford: Oxford University) pp 438
[4] Glauber R J 2006 Nobel Lecture: One Hundred Years of Light Quanta *Rev. Mod. Phys* **78** pp. 1267-1278.
[5] Miguel M S, Feng Q, and Moloney J V 1995 Light-polarization dynamics in surface-emitting semiconductor lasers *Phys. Rev. A* **52** pp. 1728-1739.
[6] Martín-Regalado J, Miguel M S, Abraham N B, and Prati F 1996 Polarization switching in quantum-well vertical-cavity surface-emitting lasers *Opt. Lett.* **21** pp. 351-353.
[7] Henry C 1982 Theory of the linewidth of semiconductor lasers *IEEE J. Quantum. Elect.* **18** pp. 259-264.