09;07.3

Generation of random sequences by switching transverse modes in a quantum cascade laser

© V.V. Dudelev[1], E.D. Cherotchenko[1], D.A. Mikhailov[1], D.V. Chistyakov[1], S.O. Slipchenko[1], A.V. Lutetskii[1], A.G. Gladyshev[2], A.V. Babichev[2], L.Ya. Karachinskii[2], I.I. Novikov[2], N.A. Pikhtin[1], A.Yu. Egorov[3], A.V. Kondrashov[4], A.A. Semenov[4], G.S. Sokolovskii[1], A.B. Ustinov[4]

[1] Ioffe Institute, St. Petersburg, Russia
[2] Connector Optics LLC, St. Petersburg, Russia
[3] Alferov Federal State Budgetary Institution of Higher Education and Science Saint Petersburg National Research Academic University of the Russian Academy of Sciences, St. Petersburg, Russia
[4] St. Petersburg State Electrotechnical University „LETI", St. Petersburg, Russia
E-mail: ustinov-rus@mail.ru

Received September 15, 2023
Revised October 2, 2023
Accepted October 2, 2023

The generation of random bit sequences by switching transverse modes in a quantum cascade laser (QCL) was studied. To receive the radiation, a quantum cascade detector (QCD) made from a QCL heterostructure was used, which provides the possibility of combining them in a photonic integrated circuit. The study was carried out for a QCL pump pulse duration of 130 ns with a repetition rate of 10−100 kHz. It is shown that electrical pulses with a randomly varying voltage value appear at the output of the QCL−QCD optical coupler. Pulses could be converted into random bit sequences using appropriate comparison.

Keywords: Integrated optics, quantum cascade laser, random bit sequences.

DOI: 10.21883/0000000000

Random sequences of numbers or bits find various applications in modern science and technology. For example, they are used to model stochastic systems and generate cryptographic keys. The operation of hardware random number generators (RNGs) relies on certain physical processes: chaotic or noise processes and instabilities of various kinds emerging in nonlinear dynamic systems. Classical examples of such processes are thermal resistor noise, shot noise in semiconductor Zener diodes or vacuum tubes, decay of radioactive materials, and instability of the oscillator generation frequency [1–4].

It was demonstrated in [5] that quantum cascade lasers (QCLs) are promising sources for RNGs to be used in secure wireless optical communication systems. The mentioned approaches provide an opportunity to achieve stable generation of random bit sequences, but the use of an external cavity and photodetectors based on cadmium−mercury−tellurium solid solutions prevents one from fabricating compact and vibration-resistant integrated-optical devices. A more promising method for generation of random sequences involves the detection of spatiotemporal non-uniformities of the output radiation intensity emerging due to multimode generation in wide-stripe semiconductor lasers [6]. The latest research into quantum cascade detector (QCD) design [7] opens up the opportunities for production of compact integrated-optical devices based on QCL−QCD optical couplers.

The results of studies into the design and fabrication of an RNG with a QCL−QCD optical coupler are reported below. A QCL and a QCD were fabricated from the same heterostructure with an active region based on an InGaAs/InAlAs heteropair (isoperiodic with an InP substrate) by two-stage epitaxial growth. The active region was formed by molecular-beam epitaxy (OOO „Konnektor Optiks"). The top InP waveguide cladding and the InGaAs contact layer were grown by metalorganic vapor phase epitaxy (Polyus Research Institute of M.F. Stelmakh). The design of the structure was discussed in detail in [8].

Postgrowth processing of heterostructures involved the following procedures performed in sequence: deposition of a photoresistive mask; etching of grooves, which formed a ridge waveguide, through the mask; deposition of a dielectric layer; contact-hole opening; and deposition of top and bottom contacts. The prepared wafer was cleaved into chips and mounted onto a copper heatsink (with the epitaxial layer facing down). The examined QCLs had a stripe width of 60 μm and a cavity length of 4.5 mm. The postgrowth processing procedure for QCDs was the same as the one for QCLs. QCDs with the epitaxial layer facing down were mounted in a similar fashion onto a copper heatsink. The length of QCD chips and the stripe width were ~ 0.5 mm and 10 μm, respectively. Thus, the width ratio of receiving and radiating apertures was 1/6. With this ratio of QCD and QCL stripe widths, radiation from just a small part of the QCL output mirror was detected. This ensured the detection of spatiotemporal non-uniformities of the QCL intensity emerging due to multimode generation.

The QCL output characteristics were examined in the pulsed mode. The duration of a pump pulses was ~ 130 ns at a repetition rate of 11.5 kHz. The typical current–voltage

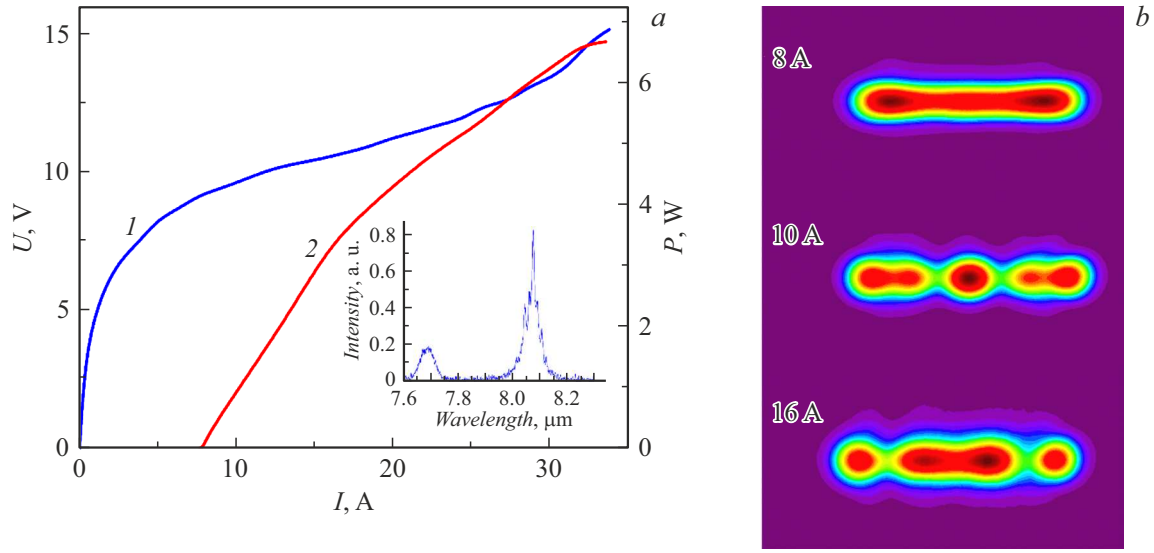

Figure 1. *a* — Typical current–voltage (*1*) and current–power (*2*) QCL curves. The power from one mirror is indicated. The typical QCL lasing spectrum at a pump current of 15 A is shown in the inset. *b* — Near-field QCL intensity distribution for the currents of 8, 10, and 16 A. The QCL was pumped by current pulses with a duration of $\sim$ 130 ns at a repetition rate of 11.5 kHz.

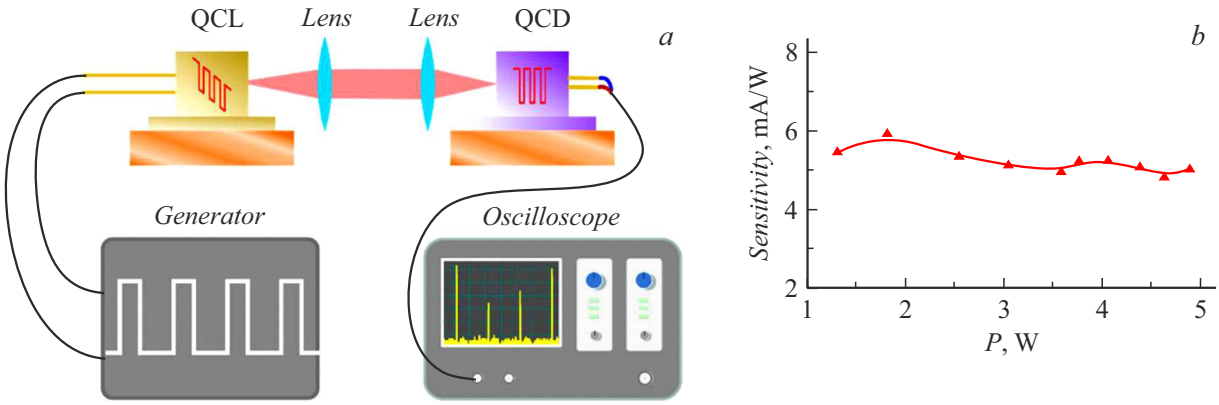

Figure 2. *a* — Block diagram of the RNG based on the QCL–QCD coupler; *b* — dependence of the QCD sensitivity on the pump power in RNG operation.

and current–power QCL curves are shown in Fig. 1, *a*. The output power is indicated for radiation from one mirror. The typical lasing spectrum is presented in the inset of Fig. 1, *a*. The maximum of this spectrum corresponds to a wavelength of 8.1 μm, which is within the atmospheric transparency window.

The spatial characteristics of QCL output radiation were examined, and the obtained results are presented in Fig. 1, *b*. A Dataray IR-BB bolometric camera was used in these experiments. The design of studies into spatial QCL characteristics was detailed in [9]. Since the frame rate of the camera is 8 Hz, the presented near-field QCL intensity distribution is an averaged one. It is evident that the number of transverse modes involved in lasing increases with increasing pump current amplitude. When the pump current goes above 14 A, the near-field pattern remains visually unchanged, suggesting that the number of transverse lasing modes has reached its maximum. An operating current of 16 A was chosen for the RNG based on the results of examination of the current-power QCL curve. The current-power curve does not reach saturation at this current level, but stable lasing with the maximum number of lateral modes is observed, providing the needed spatiotemporal non-uniformity of the QCL radiation intensity. It made no practical sense to raise the operating current further, since the signal was detected reliably and stable generation of random sequences was observed.

The diagram of the RNG based on the QCL–QCD optical coupler is shown in Fig. 2, *a*. QCL radiation was focused onto the input aperture of the photodetector by an optical system with a magnification ratio of 1. All elements of the optical system, the QCL, and the QCD were mounted on high-precision three-coordinate micropositioners with a nanometer sensitivity to ensure efficient radiation coupling

to the QCD waveguide. Emission (and absorption) associated with interband transitions in quantum wells and structures based on them (QCLs and QCDs included) is TM-polarized. Therefore, the QCD was pumped at the end to obtain the needed radiation polarization.

As was demonstrated in [6], the presence of a large number of lateral lasing modes leads to a chaotic time dependence of the radiation intensity distribution over the laser mirror. Therefore, spatial selectivity of the detection circuit is needed for an RNG to be operational. The ratio of QCD and QCL apertures in the designed optical circuit was 1/6, providing the required spatial resolution for the detection of intensity fluctuations of competing radiation modes. A current pulse generator was used to pump the QCL, which was cooled by a water-cooled thermoelectric cooling unit. The QCL was connected to an oscilloscope by a coaxial cable with a wave impedance of 50 Ω. No offset was needed to detect the QCD radiation (see the schematic diagram in Fig. 2, *a*). The QCD sensitivity was found to remain constant within the entire range of pump currents and reached ∼ 12 and 5.5 mA/W in operation with the QCL with a stripe width of 16 and 60 μm, respectively (Fig. 2, *b*). The upper power limit for radiation detected by the QCL corresponded to the maximum output power of available QCLs. A reduction in sensitivity in experiments with the QCL with a greater stripe width is attributable to the fact that the focal spot grew in size relative to the input aperture, providing the needed spatial resolution of the detection circuit, but reducing the efficiency of radiation coupling to the QCD.

Duration $\tau = 130$ ns was set for the pump current pulses.. Pulse period T was varied from 10 to 100 μs, which corresponded to repetition rate $f = 10-100$ kHz. The upper repetition rate limit was defined exclusively by the operating capabilities of the QCL driver. A Tektronix DPO 7354 real-time oscilloscope was used to measure pulse sequences. The sample rate was set to 100 Ms/s (10 ns/pt), which corresponded to 13 points per pulse. The length of oscilloscope records was 200 ms. Thus, the number of measured pulses in each oscilloscope record depended on the period and varied from 2000 to 20 000.

A typical oscilloscope record of voltage at the RNG output is shown in Fig. 3. It can be seen that the amplitude of voltage pulses varies randomly within the 0.18−0.4 V range. The experimentally measured pulse voltage varied within a certain range between its minimum and maximum values. A sequence of pulses was then sent to a comparator. Threshold comparator voltage U_t was chosen from within the range between minimum and maximum pulse voltage values.

Five tests from the NIST set of statistical tests [10] were used to verify the randomness of obtained bit sequences. Specifically, a frequency (monobit) test, a frequency test within a block, a runs test, a test for the longest run of ones in a block, and a discrete Fourier transform (spectral) test were performed. The first test determines whether a sequence has more zeros or more ones. If the numbers

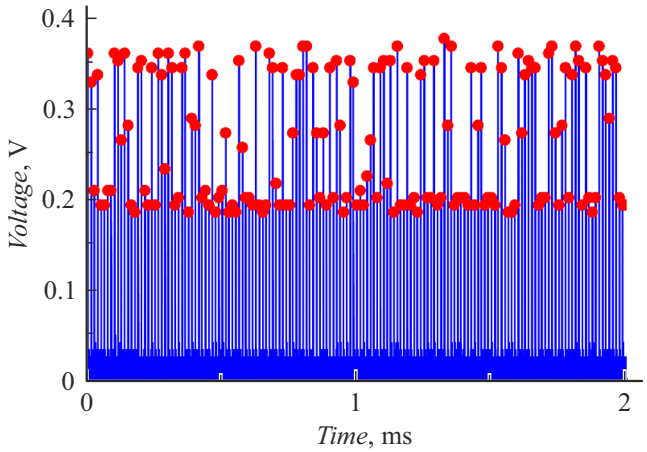

Figure 3. Typical fragment of an oscilloscope record for current pump pulse period $T = 16.7\,\mu$s.

of zeros and ones are approximately equal, the test is considered passed. The second test is similar to the first one; the difference is that individual blocks of the initial sequence are examined. The third test evaluates the number and lengths of blocks of identical bits in the examined sequence and determines whether the results are consistent with the assumption that this sequence is a truly random one. As the name implies, the fourth test finds out the maximum length of a block consisting exclusively of ones and establishes whether this length is appropriate for a random sequence. The last test uses the discrete Fourier transform to search for spectral maxima indicating the presence of recurring sections in a bit sequence. Quantity p, which is called the probability, was calculated for each test. If p exceeded 0.01, the test was considered passed. A sequence had to pass all five tests for it to be regarded as a random one.

The results of processing of time realizations and testing of the obtained sequences revealed that threshold voltage U_t at which random bit sequences are generated from the examined pulse trains falls within the range from 250 to 300 mV.

The obtained results demonstrate that wide-stripe QCLs, which are similar to laser diodes [6] in producing a multitude of lateral modes, are characterized by spatiotemporal non-uniformity (attributable to mode competition) of the radiation intensity distribution at the output mirror. This explains why the proposed generator based on the QCL−QCD optical coupler produces random bit sequences reliably. The regime of generation of electric pulses with the voltage varying within a certain range between its minimum and maximum values is the optimum one. It seem feasible to increase the generation rate by combining an array of QCDs with a wide-stripe QCL in a single photonic integrated circuit. Preliminary estimates suggest that the generation rate may then reach tens-hundreds of megahertz.

Funding

The QCL−QCD optical coupler was fabricated as part of the research program of the National Physics and Mathematics Center (project „High Energy Density Physics. Phase 2023–2025"). The experiments on generation of random bit sequences and the analysis of data were supported by a project of the St. Petersburg Electrotechnical University „LETI" within the „Priority-2030" academic leadership program.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] R.S. Maddocks, S. Matthews, E.W. Walker, C.H. Vincent, J. Phys. E, **5** (6), 542 (1972). DOI: 10.1088/0022-3735/5/6/018
[2] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo, IEEE Trans. Comput., **52** (4), 403 (2003). DOI: 10.1109/TC.2003.1190581
[3] A.B. Ustinov, A.V. Kondrashov, B.A. Kalinikos, Tech. Phys. Lett., **42** (4), 403 (2016). DOI: 10.1134/S1063785016040283.
[4] M. Herrero-Collantes, J.C. Garcia-Escartin, Rev. Mod. Phys., **89** (1), 015004 (2017). DOI: 10.1103/RevModPhys.89.015004
[5] O. Spitz, J. Wu, M. Carras, Ch.-W. Wong, F. Grillot, Sci. Rep., **9**, 4451 (2019). DOI: 10.1038/s41598-019-40861-7
[6] K. Kim, S. Bittner, Y. Zeng, S. Guazzotti, O. Hess, Q.J. Wang, H. Cao, Science, **371** (6532), 948 (2021). DOI: 10.1126/science.abc2666
[7] B. Schwarz, C.A. Wang, L. Missaggia, T.S. Mansuripur, P. Chevalier, M.K. Connors, D. McNulty, J. Cederberg, G. Strasser, F. Capasso, ACS Photon., **4** (5), 1225 (2017). DOI: 10.1021/acsphotonics.7b00133
[8] E. Cherotchenko, V. Dudelev, D. Mikhailov, G. Savchenko, D. Chistyakov, S. Losev, A. Babichev, A. Gladyshev, I. Novikov, A. Lutetskiy, D. Veselov, S. Slipchenko, D. Denisov, A. Andreev, I. Yarotskaya, K. Podgaetskiy, M. Ladugin, A. Marmalyuk, N. Pikhtin, L. Karachinsky, V. Kuchinskii, A. Egorov, G. Sokolovskii, Nanomaterials, **12** (22), 3971 (2022). DOI: 10.3390/nano12223971
[9] V.V. Dudelev, D.A. Mikhailov, V.Yu. Myl'nikov, A.V. Babichev, S.N. Losev, E.A. Kognovitskaya, A.G. Gladyshev, L.Ya. Karachincky, I.I. Novikov, D.V. Densov, S.O. Slipchenko, A.V. Lyutetskii, N.A. Pikhtin, V.I. Kuchinskii, A.Yu. Egorov, G.S. Sokolovskii, Tech. Phys. Lett., **46** (11), 1152 (2020). DOI: 10.1134/S106378502011019X.
[10] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, *A statistical test suite for random and pseudorandom number generators for cryptographic applications* (National Institute of Standards and Technology, 2010), NIST special publication 800-22 Rev. 1a. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

Translated by D.Safin