DOI: 10.22184/1993-7296.FRos.2021.15.1.70.75

Широкополосный квантовый генератор шума на основе управляемого интегрально-оптического интерферометра

В. М. Петров[1], *А. В. Шамрай*[2], *И. В. Ильичев*[2], *П. М. Агрузов*[2], *В. В. Лебедев*[2]

[1] *Национальный исследовательский университет ИТМО, Санкт-Петербург, Россия*

[2] *ФТИ им. А. Ф. Иоффе РАН, Санкт-Петербург, Россия*

Впервые продемонстрирована работа квантового генератора шума в полосе не менее 4 ГГц и с превышением квантовых шумов над классическими на величину 12–13 дБ. Впервые основной элемент такого генератора – оптический светоделитель с электрически-управляемым коэффициентом деления – выполнен в виде интегрально-оптического интерферометра Маха-Цендера на подложке из ниобата лития.

Ключевые слова: квантовые коммуникации, СВЧ интегрально-оптические модуляторы, квантовый генератор шума

Статья получена: 12.01.2021
Принята к публикации: 04.02.2021

ВВЕДЕНИЕ

Генерация шума, а также генерация последовательностей случайных чисел является основой современной цифровой экономики. Последовательности случайных чисел применяются в системах безопасности, криптографии, в научных исследованиях, генерировании QR-кодов, блокчейнов, а также в играх, т. е. во всех тех практических применениях, где задача генерации истинно случайных чисел является первостепенной. В Российской Федерации уделяется особое внимание обеспечению информационной безопасности, что

Broadband Quantum Noise Generator Based on a Controlled Integral Optical Interferometer

V. M. Petrov[1], *A. V. Shamray*[2], *I. V. Ilyichev*[2], *P. M. Agruzov*[2], *V. V. Lebedev*[2]

[1] *ITMO National Research University, St. Petersburg, Russia*

[2] *A. F. Ioffe PTI of RAS, St. Petersburg, Russia*

The work of a quantum noise generator in a band of at least 4 GHz, and with an excess of quantum noise over classical ones by 12–13 dB was demonstrated for the first time. The novel main element of such generator, an optical beam splitter with an electrically controlled splitting ratio, is made in the form of an integrated optical Mach-Zehnder interferometer on a lithium niobate substrate.

Keywords: quantum communications, microwave integrated optical modulators, quantum noise generator

Received on: 12.01.2021
Accepted on: 04.02.2021

INTRODUCTION

Generating noise as well as generating sequences of random numbers is the backbone of the modern digital economy. Sequences of random numbers are used in security systems, cryptography, scientific research, generating QR codes, blockchains, as well as in games, i. e. in all those practical applications where the task of generating truly random numbers is paramount. In the Russian Federation, special attention is paid to ensuring information security, which follows from the doctrine of "Information security of the Russian Federation", approved by Decree of the President of the Russian Federation No. 646 dated December 5, 2016.

Our recent successes [1–3] related to the creation of high-quality controllable integrated-optical devices allowed us to create a compact quantum noise generator based on an electrically controlled integrated-optical beam splitter, made according to the Mach-Zehnder interferometer scheme.

DEVELOPMENT STATUS

The idea of using a circuit of a quantum noise generator based on vacuum fluctuations (see Fig. 1), containing

следует из доктрины «Информационной безопасности Российской Федерации», утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. № 646.

Наши недавние успехи [1–3], связанные с созданием высококачественных управляемых интегрально-оптических устройств, позволили нам создать компактный квантовый генератор шума на основе интегрально-оптического светоделителя с электрическим управлением, выполненного по схеме интерферометра Маха-Цендера.

СОСТОЯНИЕ РАЗРАБОТОК

Идея использования схемы квантового генератора шума на основе вакуумных флуктуаций (рис. 1), содержащего локальный осциллятор (лазер), оптический светоделитель СД, два фотоприемника *A*, *B* и схему вычитания электрических сигналов *A*–*B* с фотоприемников (балансный детектор), хорошо известна [4, 5]. Принцип работы такого устройства основан на одном из фундаментальных явлений квантовой физики – вакуумных флуктуациях (VF) [6]. Принято считать, что прямым подтверждением существования вакуумных флуктуаций есть лэмбовский сдвиг [7] и взаимодействие Казимира [8, 9].

В литературе описаны различные практические реализации этой схемы. В работе [4] такая схема была теоретически проанализирована, и, исходя из имеющейся на тот момент элементной базы, были даны оценки возможной производительности генератора случайных чисел на ее основе – 200 Мбит/с. В работе [10] анализ аналогичной схемы дал потенциальную оценку производительности 70 Гбит/с, а ее экспериментальная реализация на объемных элементах позволила достичь ширины полосы генерации шума 1,5–2,0 ГГц. В работе [11] экспериментально продемонстрированная ширина полосы квантовой генерации белого шума составила примерно 1,9 ГГц, в работе [12] – примерно 0,4–0,5 ГГц.

Одно из главных требований, которое предъявляется к элементам такого устройства, это высокая точность и стабильность во времени коэффициента деления светоделителя. Отклонение в процессе работы коэффициента деления от соотношения 1:1 существенным образом влияет на статистические свойства генерируемого шума. В работе [13] для решения задачи управления коэффициентом деления был использован нагреватель, введенный в одно из плеч интегрально-оптического интерферометра Маха-Цендера. Это обеспечивало контролируемый фазовый сдвиг для точной подстройки

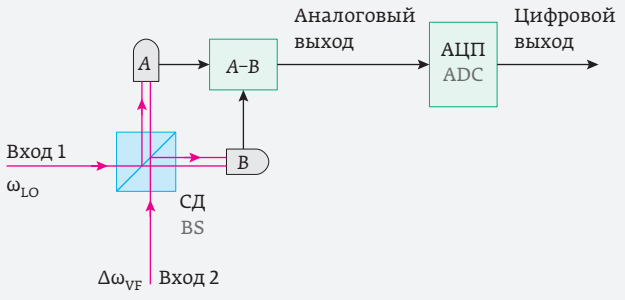

Рис. 1. *Схема квантового генератора шума на основе вакуумных флуктуаций: СД – светоделитель; A, B – фотоприемники; A-B – схема вычитания; АЦП – аналого-цифровой преобразователь (используется для получения последовательности истинно случайных чисел)*

Fig. 1. *Scheme of a quantum noise generator based on vacuum fluctuations: BS – beam splitter; A, B – photodetectors; A-B – subtraction scheme; ADC – analog-to-digital converter (used to obtain a sequence of truly random numbers)*

a local oscillator (laser), an optical beam splitter BS, two photodetectors *A*, *B* and a circuit for subtracting electrical signals *A*-*B* from photodetectors (balanced detector) is known [4, 5]. The principle of operation of such a device is based on one of the fundamental phenomena of quantum physics – vacuum fluctuations VF [6]. It is generally accepted that the Lamb shift [7] and the Casimir interaction [8, 9] are direct confirmation of the existence of vacuum fluctuations.

Practical implementations of this scheme are described in the literature. In [4], such a scheme was theoretically analyzed, and, based on the element base available at that time, estimates were given of the possible performance of a random number generator based on it – 200 Mbit/s. In [10], an analysis of a similar scheme gave a potential estimate of the performance of 70 Gb/s, and its experimental implementation on volumetric elements made it possible to achieve a noise generation bandwidth of 1.5–2.0 GHz. In [11], the experimentally demonstrated bandwidth of the quantum generation of white noise was approximately 1.9 GHz, in [12] – approximately 0.4...0.5 GHz.

One of the main requirements for the elements of such a device is a high accuracy and stability in time of the division ratio of the beam splitter. The deviation during operation of the division ratio from the 1:1 ratio significantly affects the statistical properties of the generated noise. In [13], a heater inserted into one of the arms of the Mach-Zehnder integrated-optical interferometer was used to solve the problem of controlling the division ratio.

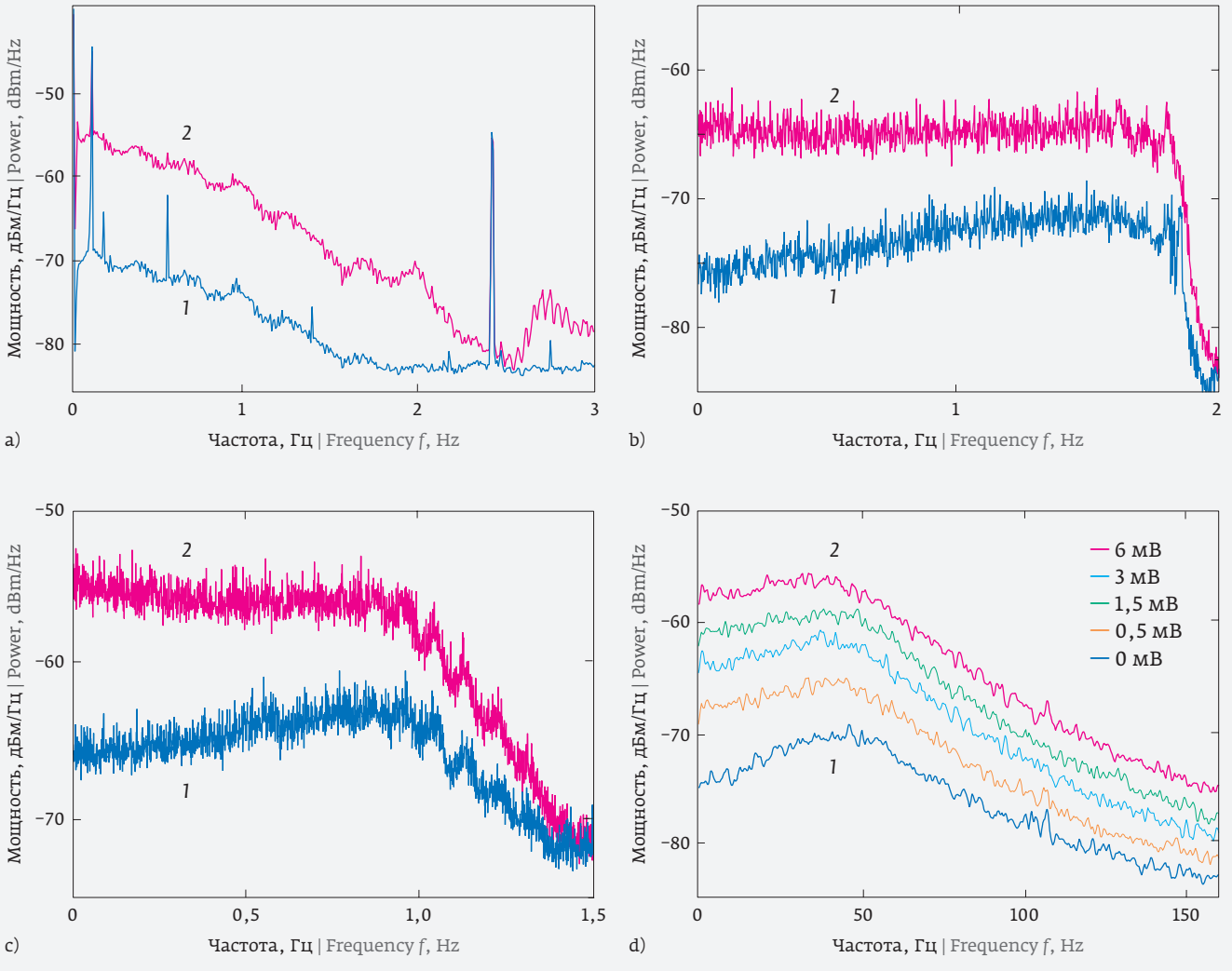

Рис. 2. *Спектр мощности электрического шума (1) и мощности электрического шума + шума вакуумных флуктуаций (2) для различных практических реализаций генератора шума (источники: a) [10]; b) [11]; c) [12]; d) [13])*

Fig. 2. *Power spectrum of electrical noise (1) and power of electrical noise + noise of vacuum fluctuations (2) for various practical implementations of the noise generator (sources: a) [10]; b) [11]; c) [12]; d) [13])*

коэффициента деления. В этом случае в качестве подложки использовался кремниевый чип. Экспериментально продемонстрированная ширина полосы генерации квантового шума в этом случае составила не более 0,1 ГГц.

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ КВАНТОВОГО ГЕНЕРАТОРА ШУМА

Нами была предложена и реализована схема квантового генератора шума, свободная от указанных выше недостатков. Схема широкополосного квантового генератора шума с электрически управляемым светоделителем в интегрально-оптическом исполнении показана на рис. 3. В качестве локального

This provided a controlled phase shift for fine tuning the division ratio. In this case, a silicon chip was used as a substrate. The experimentally demonstrated bandwidth of quantum noise generation in this case was no more than 0.1 GHz.

PRACTICAL IMPLEMENTATION OF A QUANTUM NOISE GENERATOR

We have proposed and implemented a quantum noise generator circuit free from the above disadvantages. A schematic of a broadband quantum noise generator with an electrically controlled beam splitter in an integrated-optical design is shown in Fig. 3. A semiconductor DFB laser with a wavelength of 1552 nm, a spectral

осциллятора (1) был использован полупроводниковый DFB-лазер с длиной волны 1552 нм, шириной спектра 170 кГц и мощностью 100 мВт.

Электрически управляемый светоделитель представляет из себя интегрально-оптический интерферометр Маха-Цендера с одним входом и двумя выходами (2). Волноводы (3) были изготовлены по хорошо зарекомендовавшей себя титан-диффузной технологии, обеспечивающей минимальные оптические потери в волноводах [1, 2]. Лазер (1) вместе с интегрально-оптическим светоделителем (2) и балансным фотодетектором образуют физический источник энтропии.

Одним из отличий нашего генератора является использование электро-оптического управления коэффициентом деления. Такое управление было реализовано за счет пары электродов (4), нанесенных вдоль волновода одного из плеч интерферометра. Меняя прикладываемое к электродам напряжение, можно было управлять коэффициентом деления в реальном масштабе времени с точностью не менее 0,1%.

Пара фотоприемников А и Б на основе InP, включенных как показано на рис. 3, образовывала балансный детектор (5). Чувствительность каждого фотоприемника составляла 0,78 А/Вт, темновой ток составлял менее 10 мкА. Лазер (1), светоделитель (2) и балансный детектор (5) соединены между собой стандартными оптическими волокнами с сохранением поляризации.

Аналоговый электрический сигнал с выхода балансного детектора (5) исследовался при помощи широкополосного спектроанализатора. На рис. 3 справа приведены спектры сигнала на выходе балансного детектора. Кривая (1) – локальный осциллятор выключен, кривая (2) – локальный осциллятор включен. Отсюда можно оценить ширину полосы генерации квантового шума не менее 4 ГГц.

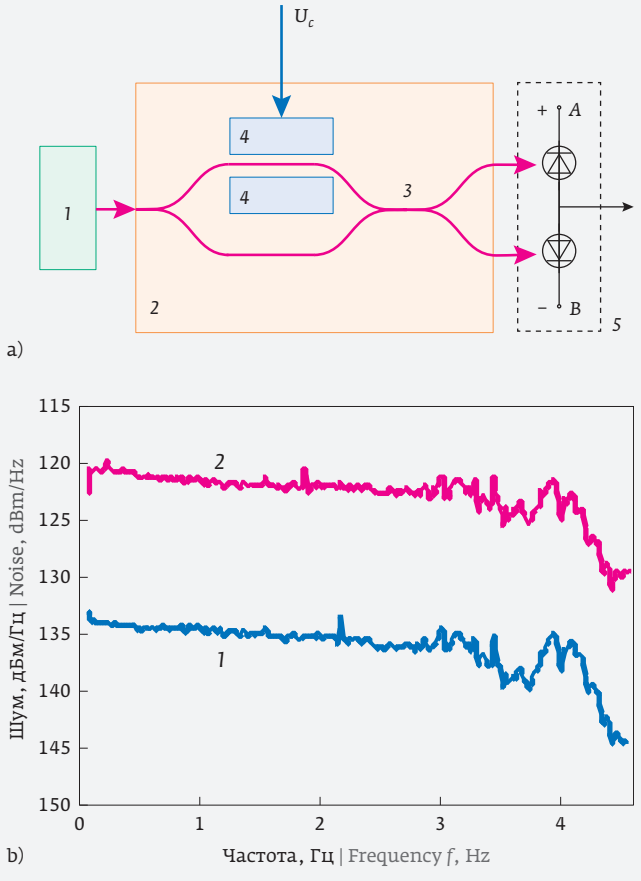

Рис. 3. *Широкополосный квантовый генератор шума с электрически-управляемым светоделителем в интегрально-оптическом исполнении: а) – схема широкополосного квантового генератора шума с электрически-управляемым коэффициентом деления (1 – локальный осциллятор (лазер); 2 – интегрально-оптический светоделитель; 3 – интерферометр Маха-Цендера; 4 – управляющие электроды; А, В – фотоприемники; 5 – балансный детектор; U_C – управляющий электрический сигнал); b) – спектр сигнала на выходе балансного детектора (кривая 1 – спектр мощности электрического шума; кривая 2 – спектр мощности электрического шума + шума вакуумных флуктуаций)*

Fig. 3. *Broadband quantum noise generator with an electrically controlled beam splitter in an integrated-optical design: a) – circuit of a broadband quantum noise generator with an electrically controlled division factor (1 – local oscillator (laser); 2 – integrated-optical beam splitter; 3 – interferometer Mach-Zehnder; 4 – control electrodes; A, B – photodetectors; 5 – balanced detector; U_C – control electrical signal); b) – spectrum of the signal at the output of the balanced detector (curve 1 is the power spectrum of electrical noise; curve 2 is the power spectrum of electrical noise + noise of vacuum fluctuations)*

ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Как следует из приведенного здесь обзора литературы, достигнутая нами ширина полосы генерации шума 4 ГГц при помощи источника энтропии, основанного на квантовых флуктуациях, на сегодняшний день является рекордной.

Для практических применений как квантовая генерация широкополосного шума, так и генерация истинно случайных последовательностей являются актуальными задачами. В данной работе мы продемонстрировали практическое решение только первой задачи – генерации широкополосного шума. Очевидно, что вторая

задача – генерация истинно случайной последовательности – может быть решена за счет использования аналого-цифрового преобразователя с необходимыми параметрами, включенного на выходе генератора шума.

Полезно оценить потенциальную производительность квантового генератора случайных чисел на основе нашего источника шума. Экспериментально измеренные значения рабочей полосы частот (~4 ГГц) и динамический диапазон (~12 дБ) дают оценку потенциальной максимальной производительности генератора случайных чисел порядка $4 \cdot 10^9 \cdot 4 = 16 \cdot 10^9$ [Гц]×[бит]. Важно отметить, что такая производительность продемонстрирована на лабораторном макете, параметры еще могут быть значительно оптимизированы.

REFERENCES

1. **Petrov V. M., Shamray A. V.** *Interferenciya i difrakciya dlya informacionnoj fotoniki.* – S.-Pb.: Lan'. 2019. 460 pp. ISBN 978-5-8114-3567-8. [In Russ.]
   Петров В. М., Шамрай А. В. *Интерференция и дифракция для информационной фотоники.* – С.-Пб.: Лань. 2019. 460 с. ISBN 978-5-8114-3567-8.
2. **Petrov V. M., Shamray A. V., Il'ichev I. V., Agruzov P. M., Lebedev V. V., Gerasimenko N. D., Gerasimenko V. S.** National Microwave Integrateed Optical Modulators for Quantum Communications. *Fotonika (Photonics Russia)*. 2020; 14 (5): 414–423. DOI: 10.22184/1993-7296. FRos.2020.14.5.414.423.[In Russ.]
   Петров В. М., Шамрай А. В., Ильичев И. В., Агрузов П. М., Лебедев В. В., Герасименко Н. Д., Герасименко В. С. Отечественные СВЧ интегрально-оптические модуляторы для квантовых коммуникаций. *Фотоника (Photonics Russia)*. 2020; 14 (5): 414–423. DOI: 10.22184/1993-7296.FRos.2020.14.5.414.423.
3. **Petrov V. M., Shamray A. V., Il'ichev I. V., Agruzov P. M., Lebedev V. V., Gerasimenko N. D., Gerasimenko V. S.** Generation of Optical Frequency Harmonics for Quantum Communication Systems at Side Frequencies. *Fotonika (Photonics Russia)*. 2020; 14(5):414–423. DOI: 10.22184/1993-7296. FRos.2020.14.5.570.582.[In Russ.]
   Петров В. М., Шамрай А. В., Ильичев И. В., Герасименко Н. Д., Герасименко В. С., Агрузов П. М., Лебедев В. В. Генерация оптических частотных гармоник для систем квантовых коммуникаций на боковых частотах. *Фотоника (Photonics Russia)*. 2020; 14 (7): 570–582. DOI: 10.22184/1993-7296.FRos.2020.14.7.570.582.
4. **Gabriel C. et al.** A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*. 2010; 4: 711–715. DOI: 10.1038/NPHOTON.2010.197.
5. **Zhou H. et al.** Randomness quantification of coherent detection. *Phys. Rev. A*. 2018; 98 (4): 042321 (7). DOI: 10.1103/PhysRevA.98.042321.
6. **Lamoreaux S. K.** The Casimir force: background, experiments, and applications. *Reports on Progress in Physics*. 2005; 68: 201–236. DOI: 10.1088/0034-4885/68/1/R04.
7. **Lamb W. E.** Fine structure of the hydrogen atom by a microwave method. *Physical Review*. 1947; 72 (3): 241–243.
8. **Petrov V., et al.** Optical detection of the Casimir Force between the macroscopic objects. *Optics Letters*. 2006; 21: 3167–3169. DOI: 10.1364/ol.31.003167
9. **Klimchitskaya G. L., et al.** Optical Chopper driven by the Casimir Force. *Phys. Rev. Applied*. 2018; 10 (1): 014010, DOI: 10.1103/PhysRevApplied.10.014010
10. **Haw J. Y. et al.** Maximization of Extractable Randomness in a Quantum Random-Number Generator. *Phys. Rev. Applied*. 2015; 3 (5): 3054004 (12). DOI: 10.1103/PhysRevApplied.3.054004.
11. **Xu B. et al.** High speed continuous variable source-independent quantum random number generation. *Quantum Sci. and Technology*. 2019; 4 (2): 025013. DOI: 10.1088/2058-9565/ab0fd9.
12. **Zheng Z. et al.** 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. *Review of Scientific Instruments*. 2019; 90 (4): 043105. DOI: 10.1063/1.5078547.
13. **Huang L., Zhou H.** Integrated Gbps quantum random number generator with

width of 170 kHz, and a power of 100 mW was used as a local oscillator (1).

An electrically controlled beam splitter is a Mach-Zehnder integrated optical interferometer with one input and two outputs (2). The waveguides (3) were manufactured using the well-proven titanium-diffusion technology, which provides minimal optical losses in the waveguides [1, 2].

The laser (1) together with the integrated optical beam splitter (2) and the balanced photodetector form a physical source of entropy.

One of the differences between our generator is the use of electro-optical control of the splitting ratio. Such control was realized due to a pair of electrodes (4) applied along the waveguide of one of the interferometer arms. By changing the voltage applied to the electrodes, it was possible to control the division ratio in real time with an accuracy of at least 0.1%.

A pair of InP photodetectors A and B, connected as shown in Fig. 3, formed a balanced detector (5). The sensitivity of each photodetector was 0.78 A/W, and the dark current was less than 10 μA. The laser (1), the beam splitter (2), and the balanced detector (5) are interconnected by standard PM optical fibers.

An analog electrical signal from the output of the balanced detector (5) was investigated using a broadband spectrum analyzer. Fig. 3, on the right, shows the signal spectra at the output of the balanced detector. Curve (1) – local oscillator is off, curve (2) – local oscillator is on. Hence, it is possible to estimate the bandwidth of quantum noise generation at least 4 GHz.

DISCUSSION OF THE RESULTS

As follows from the literature review presented here, the 4 GHz noise generation bandwidth that we have achieved using an entropy source based on quantum fluctuations is currently a record one.

For practical applications, both the quantum generation of broadband noise and the generation of truly random sequences are urgent problems. In this work, we have demonstrated a practical solution to only the first problem – the generation of broadband noise. Obviously, the second task, the generation of a truly random sequence, can be solved by using an analog-to-digital converter with the required parameters included at the output of the noise generator.

It is useful to estimate the potential performance of a quantum random number generator based on our noise source. The experimentally measured values of the operating frequency band (~4 GHz) and dynamic range (~12 dB) give an estimate of the potential maximum performance of the random number generator of the order of $4 \cdot 10^9 \cdot 4 = 16 \cdot 10^9$ [Hz]×[bit]. It is important to note that this perfor-

real-time extraction based on homodyne detection. Journal of the Optical Society of America B. 2019; 36 (3): B130–136. DOI: 10.1364/JOSAB.36.00B130.

ОБ АВТОРАХ

Петров Виктор Михайлович, д. ф.- м. н. (радиофизика), д. ф.- м. н. (оптика); e-mail: vmpetrov@itmo.ru; главный научный сотрудник, Национальный исследовательский университет ИТМО, Санкт-Петербург, Россия.
ORCID: 0000-0002-8523-0336

Шамрай Александр Валерьевич, д. ф.- м. н., e-mail: Achamrai@mail.ioffe.ru; зав. лаб. квантовой электроники ФТИ им. А. Ф. Иоффе, Санкт-Петербург, Россия.
ORCID: 0000-0003-0292-8673

Ильичев Игорь Владимирович, к. х. н., снс, лаб. квантовой электроники ФТИ им. А. Ф. Иоффе, Санкт-Петербург, Россия.
ORCID: 0000-0001-7803-0630

Агрузов Пётр Михайлович, мнс, лаб. квантовой электроники ФТИ им. А. Ф. Иоффе, Санкт-Петербург, Россия.
ORCID: 0000-0002-1248-7069

Лебедев Владимир Владимирович, к. ф.- м. н., мнс, лаб. квантовой электроники ФТИ им. А. Ф. Иоффе, Санкт-Петербург, Россия.
ORCID: 0000-0003-0292-8673

ВКЛАД ЧЛЕНОВ АВТОРСКОГО КОЛЛЕКТИВА

Статья подготовлена на основе многолетней работы всех членов авторского коллектива.

КОНФЛИКТ ИНТЕРЕСОВ

Авторы заявляют, что у них нет конфликта интересов. Все авторы приняли участие в написании статьи и дополнили рукопись в части своей работы.

mance has been demonstrated on a laboratory model; the parameters can still be significantly optimized.

ABOUT AUTHORS

Viktor Petrov, Doctor of Physical and Mathematical Sciences (Radiophysics), Doctor of Physical and Mathematical Sciences (Optics); e-mail: vmpetrov@itmo.ru; Chief Researcher, National Research University ITMO, St. Petersburg, Russia.
ORCID: 0000 0002 8523 0336

Shamray Alexander Valerievich, Doctor of Physical and Mathematical Sciences; e-mail: Achamrai@mail.ioffe.ru; Head. lab. of Quantum Electronics Physicotechnical Institute named after A. F. Ioffe, St. Petersburg, Russia.
ORCID: 0000 0003 0292 8673

Il'ichev Igor Vladimirovich, candidate of chemical sciences, senior researcher, lab. of Quantum Electronics Physicotechnical Institute named after A. F. Ioffe, St. Petersburg, Russia.
ORCID: 0000 0001 7803 0630

Agruzov Petr Mikhailovich, junior researcher, lab. of Quantum Electronics Physicotechnical Institute named after A. F. Ioffe, St. Petersburg, Russia.
ORCID: 0000 0002 1248 7069

Lebedev Vladimir Vladimirovich, junior researcher, lab. of Quantum Electronics Physicotechnical Institute named after A. F. Ioffe, St. Petersburg, Russia.
ORCID: 0000 0003 0292 8673

CONTRIBUTION BY THE MEMBERS OF THE TEAM OF AUTHORS

The article was prepared on the basis of many years of work by all members of the team of authors.

CONFLICT OF INTEREST

The authors claim that they have no conflict of interest. All authors took part in writing the article and supplemented the manuscript in part of their work.