УНИВЕРСИТЕТ ИТМО

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
ноябрь–декабрь 2021 Том 21 № 6 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
November–December 2021 Vol. 21 No 6 http://ntv.ifmo.ru/en/
ISSN 2226-1494 (print) ISSN 2500-0373 (online)

НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК УНИВЕРСИТЕТ ИТМО
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ

МАТЕМАТИЧЕСКОЕ И КОМПЬЮТЕРНОЕ МОДЕЛИРОВАНИЕ

MODELING AND SIMULATION

doi: 10.17586/2226-1494-2021-21-6-962-968
УДК 530.145

Генерация случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками

Артем Александрович Петренко[1]✉, Антон Владимирович Ковалев[2], Владислав Евгеньевич Бугров[3]

[1,2,3] Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация

[1] aapetrenko@itmo.ru✉, https://orcid.org/0000-0002-7862-971X
[2] avkovalev@itmo.ru, https://orcid.org/0000-0001-7848-8526
[3] vladislav.bougrov@itmo.ru, https://orcid.org/0000-0002-5380-645X

Аннотация

Предмет исследования. Представлены результаты исследования процесса генерации случайных битовых последовательностей с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками. **Метод.** Для моделирования лазерной генерации массива связанных микростолбиков использованы скоростные уравнения для лазеров на квантовых точках. Численное моделирование динамики массива лазеров осуществлено при помощи полуимплицитного метода Эйлера, реализованного на языке Julia. Алгоритм генерации битовой последовательности представляет собой последовательную реализацию следующих шагов: выборка значений интенсивности суммарного поля массива связанных микростолбиков, нормировка и дискретизация полученных значений в соответствии с разрешением восьмибитного аналого-цифрового преобразователя, извлечение четырех младших разрядов из битового представления дискретизированных значений, конкатенация битовых значений в единую последовательность. **Основные результаты.** Показана возможность генерации битовых последовательностей с равновероятным распределением нулей и единиц с производительностью до 400 Гбит/с при использовании массива связанных лазеров на основе микростолбиков с квантовыми точками. Полученные при частоте выборки интенсивности суммарного поля 100 гигавыборок в секунду и сохранении четырех младших разрядов последовательности длиной 14 285 716 битов успешно прошли 14 статистических тестов NIST 800-22 для *p*-значения 0,01. **Практическая значимость.** Предложенный метод может быть реализован при разработке генераторов случайных чисел на базе более масштабных массивов связанных лазеров на основе микростолбиков с квантовыми точками. Результаты работы могут найти применение при экспериментальной реализации генераторов случайных чисел с использованием массивов связанных лазеров на основе микростолбиков с квантовыми точками.

Ключевые слова

генераторы случайных чисел, микростолбики с квантовыми точками, релаксационные колебания, защищенные коммуникации

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации, проект тематики научных исследований № 2019-1442.

Ссылка для цитирования: Петренко А.А., Ковалев А.В., Бугров В.Е. Генерация случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками // Научно-технический вестник информационных технологий, механики и оптики. 2021. Т. 21, № 6. С. 962–968. doi: 10.17586/2226-1494-2021-21-6-962-968

Random number generation with arrays of coupled quantum-dot micropillar lasers

Artem A. Petrenko[1]✉, Anton V. Kovalev[2], Vladislav E. Bougrov[3]

[1,2,3] ITMO University, Saint Petersburg, 197101, Russian Federation

[1] aapetrenko@itmo.ru✉, https://orcid.org/0000-0002-7862-971X
[2] avkovalev@itmo.ru, https://orcid.org/0000-0001-7848-8526
[3] vladislav.bougrov@itmo.ru, https://orcid.org/0000-0002-5380-645X

Abstract

The paper investigates the results of random number generation with arrays of coupled quantum-dot micropillar lasers. The micropillars array laser generation is modeled based on the rate equations for quantum dot lasers. The numerical simulation of the dynamics for the arrays of coupled quantum-dot micropillar lasers is carried out utilizing the semi-implicit Euler method, implemented in Julia programming language. The algorithm of random bit sequence generation consists of the following steps: sampling the values of the total field intensity for coupled micropillar lasers; normalizing and discretizing the obtained values per resolution of the 8-bit analog-to-digital converter; extracting the four least significant bits from the bit representation of the sampled values; concatenating the bit values in a single sequence. The possibility of the bit sequences generation having an equiprobable distribution of zeros and ones with a performance of up to 400 Gbit/s was shown utilizing a random number generator based on an array of coupled quantum-dot micropillar lasers for sequences with a length of 14285716 bits at a sampling rate of 100 gigasamples per second and four least significant bits extraction. The resulting bit sequences successfully passed 14 NIST 800-22 statistical tests for the *p*-value equal to 0.01. The proposed method can be applied to develop random number generators based on larger arrays of coupled quantum-dot micropillar lasers. The results can be utilized in the experimental implementation of random number generators based on arrays of coupled quantum-dot micropillar lasers.

Keywords

random number generators, semiconductor micropillars, quantum-dot micropillars, secure communication

Acknowledgements

This work was supported by the Ministry of Science and Higher Education of Russian Federation, research project no. 2019-1442.

For citation: Petrenko A.A., Kovalev A.V., Bougrov V.E. Random number generation with arrays of coupled quantum-dot micropillar lasers. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2021, vol. 21, no. 6, pp. 962–968 (in Russian). doi: 10.17586/2226-1494-2021-21-6-962-968

Введение

Стремительная цифровизация общества и экономики играет первостепенную роль в увеличении спроса на повышение безопасности передаваемой информации, что служит дополнительным стимулом развития криптографии и защищенных коммуникаций [1]. В связи с тем, что ряд криптографических преобразований использует в качестве исходных данных некоторые первичные состояния, создаваемые генераторами случайных чисел, надежность криптографических алгоритмов определяется качеством генерируемых случайных последовательностей. Успешность применения генераторов случайных чисел опирается на способность быстро воспроизводить потоки битов, между которыми не наблюдается заметных корреляций [2].

Существующие компьютерные алгоритмы генерации псевдослучайных чисел не способны обеспечить требуемый уровень безопасности, что послужило ключевой причиной развития генераторов случайных чисел на основе физических источников энтропии [3]. В настоящий момент физические генераторы случайных чисел могут соревноваться в скорости с псевдослучайными алгоритмами, что позволяет судить об их определяющей роли при создании систем связи и вычислений с максимальной надежностью и производительностью [2, 4–6].

В последние годы наибольший интерес в области создания физических генераторов случайных чисел представляют устройства, в основе работы которых лежат квантово-механические процессы. Высокий уровень внутренней неопределенности этих процессов позволяет поддерживать генерацию случайных битов. Известны конструкции, основанные на регистрации времени детектирования одиночных фотонов [7, 8], распределении числа одиночных фотонов [9, 10], регистрации фазовых шумов [11, 12], флуктуаций вакуума [13–15], регистрации изменений интенсивности излучения лазеров [16–18]. Именно на принципе регистрации хаотических колебаний интенсивности излучения построена работа новых типов квантовых генераторов случайных чисел с использованием массивов связанных лазеров на основе микростолбиков, представляющих собой эпитаксиально выращенные планарные микрорезонаторы, обладающие богатой хаотической динамикой в силу эванесцентного сопряжения [19].

В настоящей работе представлены результаты моделирования динамики массива трех микростолбиков с квантовыми точками. Приведен алгоритм получения последовательностей битов, являющихся результатом работы генератора случайных чисел. Показана возможность воспроизведения битовых последовательностей, успешно прошедших статистические тесты на определение случайности, со скоростью до 400 Гбит/с.

Модель лазера на основе микростолбика с квантовыми точками

Выполним моделирование генератора случайных чисел при помощи скоростных уравнений для массива лазеров на основе микростолбиков с квантовыми точ-

ками, которые для одного лазера записываются следующим образом [20, 21]:

$$\dot{E}(t) = \frac{1}{2}(1 + i\alpha)[g(2\rho(t) - 1) - 1]E(t),$$
$$\dot{\rho}(t) = \eta_d[F(\rho(t),n(t)) - \rho(t) - (2\rho(t) - 1)|E(t)|^2],$$
$$\dot{n}(t) = \eta_w[J - n(t) - 2F(\rho(t),n(t))],$$

где t — время, выраженное в единицах времени жизни фотона в резонаторе (τ_p); точка «·» — дифференцирование по времени; $E(t)$ — комплексная амплитуда поля лазерного излучения; $\rho(t)$ — вероятность заселенности точки в основном состоянии; $n(t)$ — число носителей заряда в смачивающем слое; α — фактор уширения линии; g — дифференциальное усиление; η_d — отношение между временем жизни фотона и скоростью релаксации заселенности точки (τ_d); η_w — отношение между временем жизни фотона и скоростью релаксации смачивающего слоя (τ_w); J — параметр накачки.

Обмен носителями заряда между квантовой точкой и смачивающим слоем характеризуется функцией:

$$F(\rho(t), n(t)) = R^{cap}(1 - \rho(t)) - R^{esc}\rho(t),$$

где $R^{cap} = Bn(t)$ — процесс захвата носителя заряда со скоростью B порядка 10^3; R^{esc} — зависящая от температуры скорость высвобождения носителя заряда в смачивающий слой ($R^{esc} << 1$); $(1 - \rho(t))$ — слагаемое, которое учитывает принцип запрета Паули.

Оценим параметры модели, соответствующие данным эксперимента [22, 23], на основе частоты релаксационных колебаний. Для этого проведем аппроксимацию экспериментальных данных зависимостью релаксационной частоты от параметра накачки, полученной в результате линеаризации модели для стационарных решений. Примем во внимание, что экспериментально определенное значение времени жизни фотона в резонаторе составляет порядка 10 пс [23].

Значения параметров модели приведены в табл. 1, коэффициент детерминации R^2 составил 0,996 (фактор уширения линии α не приведен, так как не влияет на частоту релаксационных колебаний f_{RO} в данной модели в отсутствие оптической обратной связи). Аппроксимирующая зависимость частоты релаксационных колебаний лазера на основе микростолбика с квантовыми точками f_{RO} от превышения параметра накачки над пороговым значением при значениях параметров, приведенных в табл. 1, а также показатель подавления релаксационных колебаний для определенных при аппроксимации параметров представлены на рис. 1 (оранжевые линии).

Пороговое значение параметра накачки определяется:

$$J_{thr} = [(1 + g)(g(1 + B) - B)]/(Bg(g - 1)).$$

Таблица 1. Значения параметров модели

Table 1. Model parameters values

Параметр	Значение
Дифференциальное усиление g	1,15
Время жизни фотона τ_p, пс	7
Время релаксации заселенности точки τ_d, нс	0,1
Время релаксации смачивающего слоя τ_w, нс	0,1
Скорость захвата носителей заряда B	924
Скорость высвобождения носителя заряда в смачивающем слое R^{esc}	0

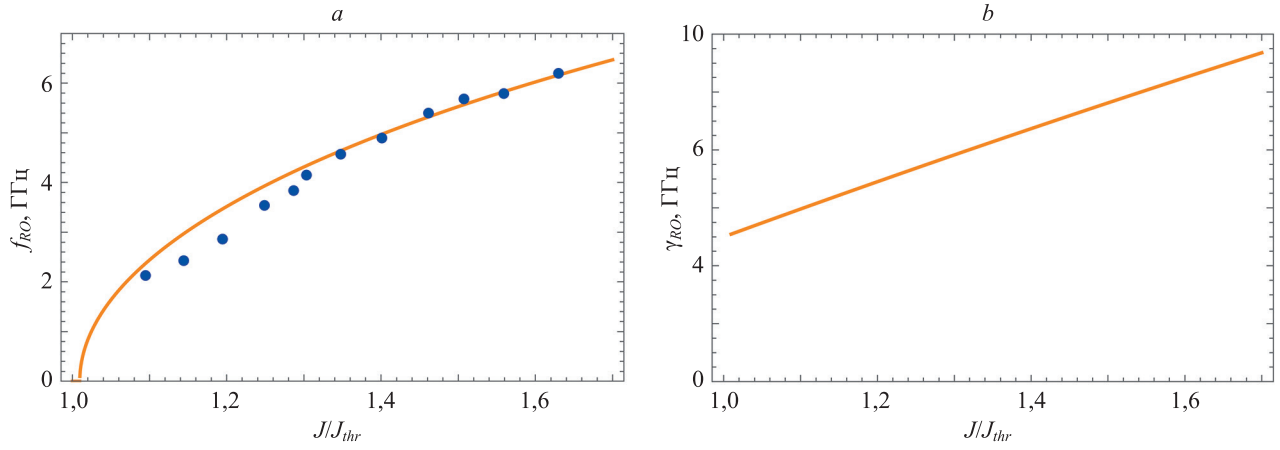

Рис. 1. Аппроксимация (оранжевая линия) экспериментальной зависимости (синие точки [22]) частоты релаксационных колебаний лазера на основе микростолбика с квантовыми точками (*a*) и соответствующий аппроксимации показатель подавления релаксационных колебаний γ_{RO} (*b*)

Fig. 1. Approximation (orange line) of the relaxation oscillations frequency experimental dependence (blue dots [22]) for the quantum-dot micropillar laser (*a*) and the relaxation oscillations suppression ratio corresponding to the approximation γ_{RO} (*b*)

Динамические режимы массива связанных лазеров на основе микростолбиков с квантовыми точками

Рассмотрим систему, состоящую из массива M сопряженных друг с другом идентичных лазеров на основе микростолбиков с квантовыми точками, для случая, когда каждый микростолбик взаимодействует только со своими соседями [24, 25]. Тогда комплексная амплитуда поля k-го столбика из данного массива может быть определена как:

$$\dot{E}_k(t) = \frac{1}{2}(1 + i\alpha)G_k(t)E_k(t) + i\kappa(E_{k-1}(t) + E_{k+1}(t)),$$

где $G_k(t) = g(2\rho_k(t) - 1) - 1$ отвечает за усиление; к — параметр связи, зависящий от эванесцентного сопряжения между микростолбиками; индекс микростолбика k определен в диапазоне от 1 до M.

Активная среда моделируется следующим образом:

$$\dot{\rho}_k(t) = \eta_d[F(\rho_k(t),n_k(t)) - \rho_k(t) - (2\rho_k(t) - 1)|E_k(t)|^2],$$

$$\dot{n}_k(t) = \eta_w[J - n_k(t) - 2F(\rho_k(t),n_k(t))].$$

Моделирование динамики трех микростолбиков осуществлено при помощи полуимплицитного метода Эйлера, реализованного на языке Julia. На рис. 2 представлена бифуркационная диаграмма, показывающая зависимость экстремумов интенсивности суммарного поля излучения лазеров и ее радиочастотного спектра от параметра связи к. Заметим, что в диапазоне к от 0,06 до 0,19 система демонстрирует хаотический режим, который может быть использован для генерации случайных чисел. Радиочастотный спектр в данном диапазоне может быть охарактеризован как плоский, что говорит о равномерном распределении всех частотных компонент в сигнале интенсивности и потенциально качественной генерации случайных чисел. Рис. 3 демонстрирует временные диаграммы, оптический и радиочастотный спектр излучения лазеров, входящих в систему, а также суммарного поля для значения к = 0,09, при котором система находится в режиме генерации развитого хаотического состояния.

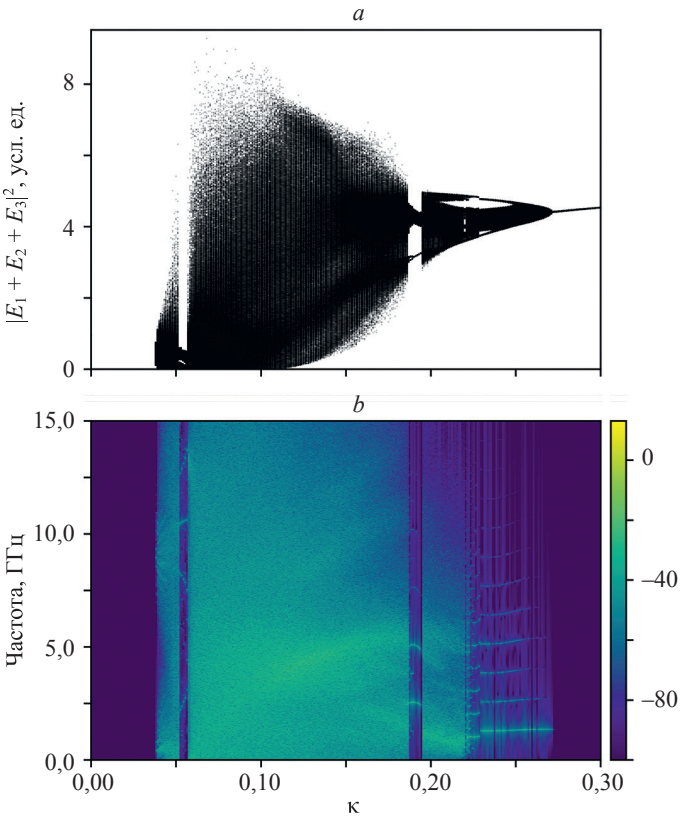

Рис. 2. Бифуркационная диаграмма (*a*) и радиочастотный спектр сигнала интенсивности (*b*) для массива связанных лазеров на основе микростолбиков с квантовыми точками при изменении параметра связи к.

Цветная шкала соответствует спектральной плотности мощности в дБ/Гц

Fig. 2. Bifurcation diagram (*a*) and the radio-frequency spectrum of intensity signal (*b*) for an array of coupled quantum-dot micropillar lasers with a change in the coupling parameter к.

The color scale corresponds to the power spectral density in dB/Hz

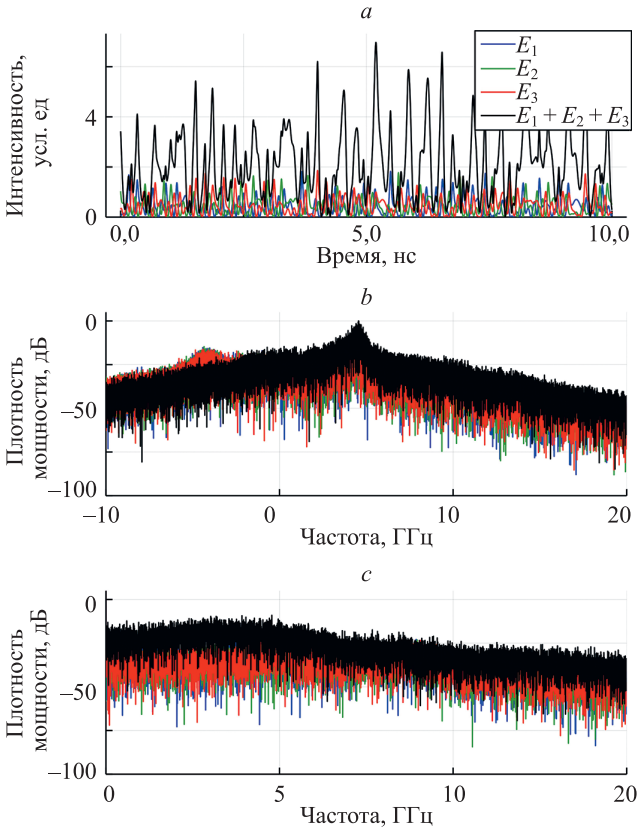

Рис. 3. Временная диаграмма интенсивности (*a*), оптический (*b*) и радиочастотный (*c*) спектры полей излучения лазеров при к = 0,09, $J = 1{,}5J_{thr}$. Частота оптического спектра определена относительно центральной частоты полосы усиления. Значение параметра α = 2

Fig. 3. Intensity time trace (*a*), optical (*b*) and radio-frequency (*c*) spectra of the laser radiation fields for к equal to 0.09, J equal to 1.5 J_{thr}. The optical spectrum frequency is determined relative to the gain band central frequency. Parameter α = 2

Генерация битовой последовательности

Для получения битовой последовательности, являющейся результатом работы генератора случайных чисел на базе массивов связанных лазеров на основе микростолбиков, при моделировании использовался следующий алгоритм:

1) задается частота, с которой осуществляется выборка значений интенсивности суммарного поля $|E_1 + E_2 + E_3|^2$;
2) полученные значения нормируются и дискретизируются в соответствии с разрешением аналого-цифрового преобразователя (было принято равным 8 бит, что соответствует 256 уровням);
3) дискретизированные значения интенсивности из диапазона 0–255 переводятся в битовое представление;
4) для каждого битового представления выбираются четыре младших разряда;
5) осуществляется конкатенация полученных битовых значений в итоговую битовую последовательность.

Анализ выполнен для значений параметра связи к равного 0,05; 0,09; 0,12; 0,15; 0,21 с целью подтверждения качества генерации случайных чисел при хаотическом режиме работы (остальные параметры соответствуют рис. 3). Для получения всех последовательностей смоделирована интенсивность суммарного поля в течение 35 мкс. Далее с частотой выборки 100 гигавыборок в секунду получены битовые последовательности длиной 14 285 716 бит, и определена вероятность появления нулей, которая составила 0,441; 0,498; 0,500; 0,500; 0,506 соответственно. При выборе четырех младших разрядов для получения последовательностей скорость генерации случайных чисел составила 400 Гбит/с.

На следующем этапе осуществлена проверка последовательности на случайность при помощи статистических тестов NIST 800-22, реализованных на языке Python [26], результаты проверки приведены в табл. 2. Тест считается успешно пройденным, если *p*-значение превышает 0,01.

Из табл. 2 видно, что все тесты были успешно пройдены сгенерированными последовательностями в случаях значений параметра к равного 0,09; 0,12; 0,15, что соответствует хаотическому режиму. При к = 0,05 система находится в сложном динамическом режиме, не являющимся хаотическим. При к = 0,21 состояние близко к хаотическому, что подтверждается тем, что данная последовательность прошла большинство тестов. Таким образом, при значениях параметра связи к от 0,09 до 0,15 возможна генерация последовательностей случайных битов системой из трех связанных лазеров на основе микростолбиков с квантовыми точками.

Таблица 2. Результаты проверки битовой последовательности на случайность

Table 2. The results of randomness tests for the bit sequence

Наименование теста [26]	*p*-значение				
	к = 0,05	к = 0,09	к = 0,12	к = 0,15	к = 0,21
Частотный побитовый тест / Frequency Test (Monobit)	0,000*	0,645	0,682	0,646	0,210
Частотный блочный тест / Frequency Test within a Block	0,000*	0,330	0,624	0,782	0,302
Тест серий / Run Test	0,000*	0,103	0,833	0,599	0,002*
Тест на длиннейшую серию единиц в блоке / Longest Run of Ones in a Block	0,902	0,135	0,877	0,954	0,430
Тест рангов бинарных матриц / Binary Matrix Rank Test	0,272	0,737	0,851	0,833	0,658
Спектральный тест на основе дискретного преобразования Фурье / Discrete Fourier Transform (Spectral) Test	0,790	0,030	0,486	0,876	0,660
Тест на совпадение неперекрывающихся шаблонов / Non-Overlapping Template Matching Test	0,000*	0,709	0,263	0,829	0,441
Тест на совпадение перекрывающихся шаблонов / Overlapping Template Matching Test	0,016	0,681	0,818	0,087	0,053
Универсальный тест Маурера / Maurer's Universal Statistical test	0,000*	0,940	0,016	0,854	0,954
Тест на линейную сложность / Linear Complexity Test	0,330	0,271	0,486	0,738	0,917
Тест на периодичность / Serial test	0,000*	0,458	0,483	0,357	0,000*
	0,000*	0,514	0,648	0,481	0,000*
Тест приблизительной энтропии / Approximate Entropy Test	0,000*	0,674	0,694	0,042	0,000*
Тест кумулятивных сумм (прямой) / Cumulative Sums (Forward) Test	0,000*	0,668	0,547	0,930	0,114
Тест кумулятивных сумм (обратный) / Cumulative Sums (Reverse) Test	0,000*	0,990	0,788	0,777	0,341

* Отмечены не пройденные соответствующей последовательностью тесты.

Заключение

Представлена модель генерации массива связанных лазеров на основе микростолбиков с квантовыми точками, определен диапазон параметра связи, при котором система демонстрирует хаотический режим генерации. Предложен алгоритм получения битовой последовательности. Показано, что система, состоящая из трех связанных лазеров на основе микростолбиков, способна генерировать случайную последовательность битов с равновероятным распределением нулей и единиц с производительностью 400 Гбит/с. Полученные результаты могут быть использованы при разработке генераторов случайных чисел на базе более масштабных массивов связанных лазеров на основе микростолбиков с квантовыми точками. В дальнейшем запланирована экспериментальная реализация генераторов случайных чисел с использованием массивов связанных лазеров на основе микростолбиков с квантовыми точками.

Литература

1. Virte M., Mercier E., Thienpont H., Panajotov K., Sciamanna M. Physical random bit generation from chaotic solitary laser diode // Optics Express. 2014. V. 22. N 14. P. 17271–17280. https://doi.org/10.1364/OE.22.017271
2. Butler T., Durkan C., Goulding D., Slepneva S., Kelleher B., Hegarty S.P., Huyet G. Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser // Optics Letters. 2016. V. 41. N 2. P. 388–391. https://doi.org/10.1364/OL.41.000388
3. Huang W., Zhang Y., Zheng Z., Li Y., Xu B., Yu S. Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator // Physical Review A. 2020. V. 102. N 1. P. 012422. https://doi.org/10.1103/PhysRevA.102.012422
4. Oliver N., Soriano M.C., Sukow D.W., Fischer I. Fast random bit generation using a chaotic laser: approaching the information theoretic limit // IEEE Journal of Quantum Electronics. 2013. V. 49. N 11. P. 910–918. https://doi.org/10.1109/JQE.2013.2280917
5. Zhang L., Pan B., Chen G., Guo L., Lu D., Zhao L., Wang W. 640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser // Scientific Reports. 2017. V. 7. P. 45900. https://doi.org/10.1038/srep45900
6. Cao G., Zhang L., Huang X., Hu W., Yang X. 16.8 Tb/s true random number generator based on amplified spontaneous emission // IEEE Photonics Technology Letters. 2021. V. 33. N 14. P. 699–702. https://doi.org/10.1109/LPT.2021.3088156
7. Wahl M., Leifgen M., Berlin M., Röhlicke T., Rahn H.-J., Benson O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements // Applied Physics Letters. 2011. V. 98. N 17. P. 171105. https://doi.org/10.1063/1.3578456
8. Nie Y.Q., Zhang H.F., Zhang Z., Wang J., Ma X., Zhang J., Pan J.W. Practical and fast quantum random number generation based on photon arrival time relative to external reference // Applied Physics Letters. 2014. V. 104. N 5. P. 051110. https://doi.org/10.1063/1.4863224
9. Ren M., Wu E., Liang Y., Jian Y., Wu G., Zeng H. Quantum random-number generator based on a photon-number-resolving detector // Physical Review A. 2011. V. 83. N 2. P. 023820. https://doi.org/10.1103/PhysRevA.83.023820
10. Applegate M.J., Thomas O., Dynes J.F., Yuan Z.L., Ritchie D.A., Shields A J. Efficient and robust quantum random number generation by photon number detection // Applied Physics Letters. 2015. V. 107. N 7. P. 071106. https://doi.org/10.1063/1.4928732
11. Guo H., Tang W., Liu Y., Wei W. Truly random number generation based on measurement of phase noise of a laser // Physical Review E. 2010. V. 81. N 5. P. 051137. https://doi.org/10.1103/PhysRevE.81.051137
12. Qi B., Chi Y.M., Lo H.K., Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser // Optics Letters. 2010. V. 35. N 3. P. 312–314. https://doi.org/10.1364/OL.35.000312
13. Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U.L., Marquardt C., Leuchs G. A generator for unique quantum random numbers based on vacuum states // Nature Photonics. 2010. V. 4. N 10. P. 711–715. https://doi.org/10.1038/nphoton.2010.197
14. Zheng Z., Zhang Y., Huang W., Yu S., Guo H. 6 Gbps real-time optical quantum random number generator based on vacuum

References

1. Virte M., Mercier E., Thienpont H., Panajotov K., Sciamanna M. Physical random bit generation from chaotic solitary laser diode. *Optics Express*, 2014, vol. 22, no. 14, pp. 17271–17280. https://doi.org/10.1364/OE.22.017271
2. Butler T., Durkan C., Goulding D., Slepneva S., Kelleher B., Hegarty S.P., Huyet G. Optical ultrafast random number generation at 1 Tb/s using a turbulent semiconductor ring cavity laser. *Optics Letters*, 2016, vol. 41, no. 2, pp. 388–391. https://doi.org/10.1364/OL.41.000388
3. Huang W., Zhang Y., Zheng Z., Li Y., Xu B., Yu S. Practical security analysis of a continuous-variable quantum random-number generator with a noisy local oscillator. *Physical Review A*, 2020, vol. 102, no. 1, pp. 012422. https://doi.org/10.1103/PhysRevA.102.012422
4. Oliver N., Soriano M.C., Sukow D.W., Fischer I. Fast random bit generation using a chaotic laser: approaching the information theoretic limit. *IEEE Journal of Quantum Electronics*, 2013, vol. 49, no. 11, pp. 910–918. https://doi.org/10.1109/JQE.2013.2280917
5. Zhang L., Pan B., Chen G., Guo L., Lu D., Zhao L., Wang W. 640-Gbit/s fast physical random number generation using a broadband chaotic semiconductor laser. *Scientific Reports*, 2017, vol. 7, pp. 45900. https://doi.org/10.1038/srep45900
6. Cao G., Zhang L., Huang X., Hu W., Yang X. 16.8 Tb/s true random number generator based on amplified spontaneous emission. *IEEE Photonics Technology Letters*, 2021, vol. 33, no. 14, pp. 699–702. https://doi.org/10.1109/LPT.2021.3088156
7. Wahl M., Leifgen M., Berlin M., Röhlicke T., Rahn H.-J., Benson O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, 2011, vol. 98, no. 17, pp. 171105. https://doi.org/10.1063/1.3578456
8. Nie Y.Q., Zhang H.F., Zhang Z., Wang J., Ma X., Zhang J., Pan J.W. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Applied Physics Letters*, 2014, vol. 104, no. 5, pp. 051110. https://doi.org/10.1063/1.4863224
9. Ren M., Wu E., Liang Y., Jian Y., Wu G., Zeng H. Quantum random-number generator based on a photon-number-resolving detector. *Physical Review A*, 2011, vol. 83, no. 2, pp. 023820. https://doi.org/10.1103/PhysRevA.83.023820
10. Applegate M.J., Thomas O., Dynes J.F., Yuan Z.L., Ritchie D.A., Shields A J. Efficient and robust quantum random number generation by photon number detection. *Applied Physics Letters*, 2015, vol. 107, no. 7, pp. 071106. https://doi.org/10.1063/1.4928732
11. Guo H., Tang W., Liu Y., Wei W. Truly random number generation based on measurement of phase noise of a laser. *Physical Review E*, 2010, vol. 81, no. 5, pp. 051137. https://doi.org/10.1103/PhysRevE.81.051137
12. Qi B., Chi Y.M., Lo H.K., Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters*, 2010, vol. 35, no. 3, pp. 312–314. https://doi.org/10.1364/OL.35.000312
13. Gabriel C., Wittmann C., Sych D., Dong R., Mauerer W., Andersen U.L., Marquardt C., Leuchs G. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 2010, vol. 4, no. 10, pp. 711–715. https://doi.org/10.1038/nphoton.2010.197
14. Zheng Z., Zhang Y., Huang W., Yu S., Guo H. 6 Gbps real-time optical quantum random number generator based on vacuum

fluctuation // Review of Scientific Instruments. 2019. V. 90. N 4. P. 043105. https://doi.org/10.1063/1.5078547
15. Haw J.Y., Assad S.M., Lance A.M., Ng N.H.Y., Sharma V., Lam P.K., Symul T. Maximization of extractable randomness in a quantum random-number generator // Physical Review Applied. 2015. V. 3. N 5. P. 054004. https://doi.org/10.1103/PhysRevApplied.3.054004
16. Nguimdo R.M., Verschaffelt G., Danckaert J., Leijtens X., Bolk J., Van der Sande G. Fast random bits generation based on a single chaotic semiconductor ring laser // Optics Express. 2012. V. 20. N 27. P. 28603–28613. https://doi.org/10.1364/OE.20.028603
17. Sciamanna M., Shore K.A. Physics and applications of laser diode chaos // Nature Photonics. 2015. V. 9. N 3. P. 151–162. https://doi.org/10.1038/nphoton.2014.326
18. Kanter I., Aviad Y., Reidler I., Cohen E., Rosenbluh M. An optical ultrafast random bit generator // Nature Photonics. 2010. V. 4. N 1. P. 58–61. https://doi.org/10.1038/nphoton.2009.235
19. Gies C., Reitzenstein S. Quantum dot micropillar lasers // Semiconductor Science and Technology. 2019. V. 34. N 7. P. 073001. https://doi.org/10.1088/1361-6641/ab1551
20. Erneux T., Viktorov E.A., Mandel P. Time scales and relaxation dynamics in quantum-dot lasers // Physical Review A. 2007. V. 76. N 2. P. 023819. https://doi.org/10.1103/PhysRevA.76.023819
21. Lang R., Kobayashi K. External optical feedback effects on semiconductor injection laser properties // IEEE Journal of Quantum Electronics. 1980. V. 16. N 3. P. 347–355. https://doi.org/10.1109/JQE.1980.1070479
22. Holzinger S., Schneider C., Höfling S., Porte X., Reitzenstein S. Quantum-dot micropillar lasers subject to coherent time-delayed optical feedback from a short external cavity // Scientific Reports. 2019. V. 9. P. 631. https://doi.org/10.1038/s41598-018-36599-3
23. Kreinberg S., Porte X., Schicke D., Lingnau B., Schneider C., Höfling S., Kanter I., Lüdge K., Reitzenstein S. Mutual coupling and synchronization of optically coupled quantum-dot micropillar lasers at ultra-low light levels // Nature Communications. 2019. V. 10. N 1. P. 1539. https://doi.org/10.1038/s41467-019-09559-2
24. Kozyreff G., Vladimirov A.G., Mandel P. Global coupling with time delay in an array of semiconductor lasers // Physical Review Letters. 2000. V. 85. N 18. P. 3809–3812. https://doi.org/10.1103/PhysRevLett.85.3809
25. Alfaro-Bittner K., Barbay S., Clerc M.G. Pulse propagation in a 1D array of excitable semiconductor lasers // Chaos. 2020. V. 30. N 8. P. 083136. https://doi.org/10.1063/5.0006195
26. Kho Ang S. NIST Randomness Testsuit [Электронный ресурс]. URL: https://github.com/stevenang/randomness_testsuite, свободный. Яз. англ. (дата обращения: 01.09.2021).

fluctuation. *Review of Scientific Instruments*, 2019, vol. 90, no. 4, pp. 043105. https://doi.org/10.1063/1.5078547
15. Haw J.Y., Assad S.M., Lance A.M., Ng N.H.Y., Sharma V., Lam P.K., Symul T. Maximization of extractable randomness in a quantum random-number generator. *Physical Review Applied*, 2015, vol. 3, no. 5, pp. 054004. https://doi.org/10.1103/PhysRevApplied.3.054004
16. Nguimdo R.M., Verschaffelt G., Danckaert J., Leijtens X., Bolk J., Van der Sande G. Fast random bits generation based on a single chaotic semiconductor ring laser. *Optics Express*, 2012, vol. 20, no. 27, pp. 28603–28613. https://doi.org/10.1364/OE.20.028603
17. Sciamanna M., Shore K.A. Physics and applications of laser diode chaos. *Nature Photonics*, 2015, vol. 9, no. 3, pp. 151–162. https://doi.org/10.1038/nphoton.2014.326
18. Kanter I., Aviad Y., Reidler I., Cohen E., Rosenbluh M. An optical ultrafast random bit generator. *Nature Photonics*, 2010, vol. 4, no. 1, pp. 58–61. https://doi.org/10.1038/nphoton.2009.235
19. Gies C., Reitzenstein S. Quantum dot micropillar lasers. *Semiconductor Science and Technology*, 2019, vol. 34, no. 7, pp. 073001. https://doi.org/10.1088/1361-6641/ab1551
20. Erneux T., Viktorov E.A., Mandel P. Time scales and relaxation dynamics in quantum-dot lasers. *Physical Review A*, 2007, vol. 76, no. 2, pp. 023819. https://doi.org/10.1103/PhysRevA.76.023819
21. Lang R., Kobayashi K. External optical feedback effects on semiconductor injection laser properties. *IEEE Journal of Quantum Electronics*, 1980, vol. 16, no. 3, pp. 347–355. https://doi.org/10.1109/JQE.1980.1070479
22. Holzinger S., Schneider C., Höfling S., Porte X., Reitzenstein S. Quantum-dot micropillar lasers subject to coherent time-delayed optical feedback from a short external cavity. *Scientific Reports*, 2019, vol. 9, pp. 631. https://doi.org/10.1038/s41598-018-36599-3
23. Kreinberg S., Porte X., Schicke D., Lingnau B., Schneider C., Höfling S., Kanter I., Lüdge K., Reitzenstein S. Mutual coupling and synchronization of optically coupled quantum-dot micropillar lasers at ultra-low light levels. *Nature Communications*, 2019, vol. 10, no. 1, pp. 1539. https://doi.org/10.1038/s41467-019-09559-2
24. Kozyreff G., Vladimirov A.G., Mandel P. Global coupling with time delay in an array of semiconductor lasers. *Physical Review Letters*, 2000, vol. 85, no. 18, pp. 3809–3812. https://doi.org/10.1103/PhysRevLett.85.3809
25. Alfaro-Bittner K., Barbay S., Clerc M.G. Pulse propagation in a 1D array of excitable semiconductor lasers. *Chaos*, 2020, vol. 30, no. 8, pp. 083136. https://doi.org/10.1063/5.0006195
26. Kho Ang S. *NIST Randomness Testsuit*. Available at: https://github.com/stevenang/randomness_testsuite (accessed: 01.09.2021).

Авторы

Петренко Артем Александрович — ассистент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 57210121963, https://orcid.org/0000-0002-7862-971X, aapetrenko@itmo.ru
Ковалев Антон Владимирович — кандидат физико-математических наук, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 56205289400, https://orcid.org/0000-0001-7848-8526, avkovalev@itmo.ru
Бугров Владислав Евгеньевич — доктор физико-математических наук, профессор, директор Института перспективных систем передачи данных, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, SC 8321276100, https://orcid.org/0000-0002-5380-645X, vladislav.bougrov@itmo.ru

Authors

Artem A. Petrenko — Assistant, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 57210121963, https://orcid.org/0000-0002-7862-971X, aapetrenko@itmo.ru
Anton V. Kovalev — PhD, Associate Professor, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 56205289400, https://orcid.org/0000-0001-7848-8526, avkovalev@itmo.ru

Vladislav E. Bougrov — D.Sc., Full Professor, Head of the Institute of Advanced Data Transfer Systems, ITMO University, Saint Petersburg, 197101, Russian Federation, SC 8321276100, https://orcid.org/0000-0002-5380-645X, vladislav.bougrov@itmo.ru

Статья поступила в редакцию 27.09.2021
Одобрена после рецензирования 05.10.2021
Принята к печати 28.11.2021

Received 27.09.2021
Approved after reviewing 05.10.2021
Accepted 28.11.2021