Оптический журнал
Физическая оптика

DOI: 10.17586/1023-5086-2022-89-09-03-10
УДК 621.315.592

Моделирование генератора случайных чисел на основе полупроводниковых наногетероструктур с квантовыми точками с оптической обратной связью

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

Университет ИТМО, Санкт-Петербург, Россия

[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. Моделирование процесса генерации последовательностей случайных битов с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками с оптической обратной связью, реализованной в виде зеркала, расположенного на некотором расстоянии от массива. Модель массива связанных лазеров на основе микростолбиков основана на скоростных уравнениях для лазеров на квантовых точках с учетом глобальной оптической обратной связи. **Цель работы.** Аналитическое моделирование процесса работы генератора случайных чисел с использованием массива связанных лазеров на основе микростолбиков с квантовыми точками. **Метод.** Моделирование динамики осуществлено посредством численного интегрирования системы дифференциальных уравнений с использованием полуимплицитного метода Эйлера, реализованного на языке Julia. Для генерации последовательностей случайных битов использован алгоритм, включающий в себя выборку значений интенсивности суммарного поля массива, нормировку и дискретизацию с разрешением 12 бит, перевод дискретизированных значений в битовое представление, выбор 4 младших разрядов, конкатенацию битовых значений в итоговую последовательность. **Основные результаты.** Смоделирован процесс генерации последовательностей случайных битов со скоростью 400 Гбит/с, отвечающих критериям статистических тестов NIST 800-22 для p-значения 0,01, при частоте выборки интенсивности суммарного поля массива 100 гигавыборок в секунду, длине последовательности 11142860 битов. Проведен бифуркационный анализ модели массива связанных лазеров на основе микростолбиков с квантовыми точками с оптической обратной связью. Показано присутствие следа времени запаздывания обратной связи в хаотическом сигнале интенсивности излучения, которое, однако, не влияет на качество генерации случайных чисел. **Практическая значимость.** Показано, что воздействие оптической обратной связи приводит к хаотической генерации массива лазеров на основе микростолбиков с квантовыми точками, что может быть использовано для генерации случайных чисел.

Ключевые слова: генератор случайных чисел, микростолбики с квантовыми точками, лазеры с внешней обратной оптической связью, бифуркационный анализ

Благодарность: 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. Моделирование генератора случайных чисел на основе полупроводниковых наногетероструктур с квантовыми точками с оптической обратной связью // Оптический журнал. 2022. Т. 89. № 9. С. 3–10. DOI: 10.17586/1023-5086-2022-89-09-03-10

Код OCIS: 140.5960

ВВЕДЕНИЕ

Стремительное увеличение спроса на цифровизацию, сопряженное с необходимостью повышения безопасности передаваемой информации, в настоящий момент выступает стимулом к применению истинно случайных последовательностей в различных областях науки и техники, таких как сфера связи, информационных технологий, криптография, распределенные вычисления [1–3]. Истинно случайными последовательностями называют последовательности статистически не зависимых друг от друга величин, принимающих в результате эксперимента одно из заранее не предсказуемых значений. При этом распределение получаемых значений должно носить равномерный характер [4]. Для генерации истинно случайных последовательностей в генераторах случайных чисел применяются недетерминированные источники (источники энтропии) и специализированные алгоритмы постобработки, используемые для повышения качества последовательностей и исключения следов возможных детерминированных событий [5].

В области создания генераторов истинно случайных чисел в настоящее время значительный интерес представляют оптические устройства, в том числе лазеры [6–9]. В основе работы подобных генераторов случайных чисел лежит регистрация хаотических изменений интенсивности излучения [10]. Использование дополнительной петли обратной связи обеспечивает возможность реализации различных динамических сценариев, приводящих к хаотичности выходного сигнала лазера в достаточно широкой полосе частот за счет масштабирования временно́й задержки, связанной с временем обхода резонатора, относительно внутренни́х временны́х масштабов лазера, а также чувствительности фазы к возвращаемому полю [11].

При создании новых типов физических генераторов случайных чисел могут быть использованы излучающие элементы, представляющие собой лазеры на основе микростолбиков (МкС), отличающиеся богатой нелинейной хаотической динамикой [12, 13]. Динамическое поведение моделей массивов связанных лазеров на основе полупроводниковых МкС с квантовыми точками (КТ) в отсутствие глобальной оптической обратной связи было исследовано ранее [14].

В настоящей работе проведен бифуркационный анализ модели массива связанных лазеров на основе МкС с КТ с оптической обратной связью. Приведены результаты моделирования процесса генерации последовательностей случайных битов, являющихся результатом работы генератора случайных чисел, со скоростью 400 Гбит/с.

Таким образом, целью работы является аналитическое моделирование процесса работы генератора случайных чисел с использованием массива связанных лазеров на основе МкС с КТ. В ходе дальнейших исследований интерес представляет анализ динамических сценариев моделей, учитывающих присутствие оптической обратной связи.

МОДЕЛЬ МАССИВА ЛАЗЕРОВ НА ОСНОВЕ МИКРОСТОЛБИКОВ С КВАНТОВЫМИ ТОЧКАМИ С ВНЕШНЕЙ ОПТИЧЕСКОЙ ОБРАТНОЙ СВЯЗЬЮ

Рассматриваемая в настоящей работе система (рис. 1) представляет собой двумерный массив вертикально-излучающих лазеров на основе МкС с КТ, напротив которого на некотором расстоянии установлено частично-прозрачное зеркало, обеспечивающее обратную оптическую связь с запаздыванием по времени (иными словами, формирующее внешний резонатор

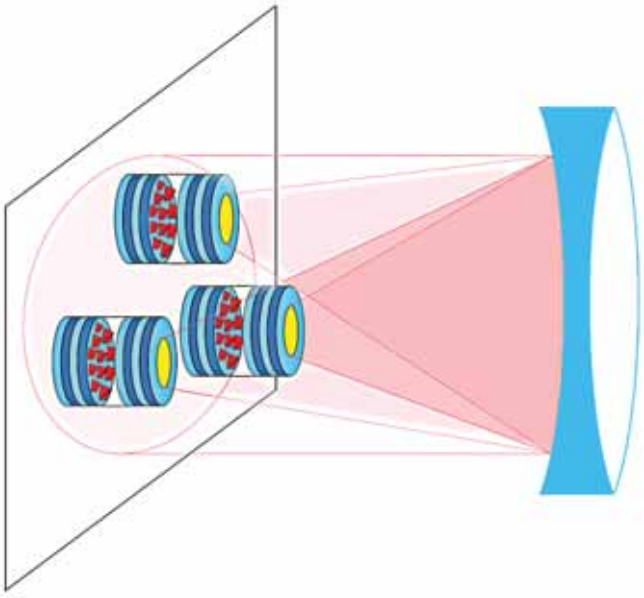

Рис. 1. Схема массива лазеров на основе микростолбиков с квантовыми точками с глобальной обратной оптической связью. Пояснения в тексте

лазера). Предполагается, что данная оптическая связь является глобальной, и иначе как посредством нее лазеры друг с другом не взаимодействуют.

Моделирование процесса генерации случайных чисел системой, состоящей из массива M связанных лазеров на основе МкС с КТ с глобальной обратной оптической связью, проводится при использовании скоростных уравнений [15]. Для k-го лазера из массива система уравнений записывается следующим образом:

$$\dot{E}_k(t) = \left[i\Delta_k + 1/2(1+i\alpha)G_k(t)\right]E_k(t) + i\gamma\sum_{j=1}^{M}\exp(-i\varphi_j)E_j(t-\tau), \quad (1)$$

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

$$\dot{n}_k(t) = \eta_w\left[J - n_k(t) - 2F(\rho_k(t),n_k(t))\right], \quad (3)$$

где t — время, выраженное в единицах времени жизни фотона в резонаторе (τ_p), $E_k(t)$ — нормированная комплексная амплитуда поля лазерного излучения k-го лазера на основе МкС, $G_k(t) = g(2\rho_k(t) - 1) - 1$ — функция, отвечающая за усиление, α — фактор уширения линии, g — дифференциальное усиление, γ — коэффициент силы обратной связи, φ_j — фазовый набег между электромагнитным полем в резонаторе и электромагнитным полем j-го лазера на основе МкС, отраженным от зеркала ($j = 1, ..., M$), τ — время обхода внешнего резонатора, Δ_k — значение расстройки между частотой излучения k-го лазера на основе МкС и опорной частотой выбранной системы координат, $\rho_k(t)$ — вероятность заселенности точки в основном состоянии, $n_k(t)$ — нормированная плотность носителей заряда в смачивающем слое, 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 — нормированный параметр накачки; точкой обозначено дифференцирование по времени.

Обмен носителями заряда между КТ и смачивающим слоем может быть охарактеризован функцией

$$F(\rho(t),n(t)) = R^{cap}(1-\rho(t)) - R^{esc}\rho(t), \quad (4)$$

где $R^{cap} = Bn(t)$ — процесс захвата носителя заряда со скоростью B порядка 10^2, R^{esc} — зависящая от температуры скорость высвобождения носителя заряда в смачивающий слой ($R^{esc} << 1$, в настоящей работе $R^{esc} = 0$), член $(1 - \rho(t))$ учитывает принцип запрета Паули.

В ходе моделирования были использованы значения параметров, соответствующие данным эксперимента [12, 16] с лазерами на основе МкС с КТ, приведенные в табл. 1. Время запаздывания 0,7 нс, что соответствует расстоянию до внешнего зеркала, равному 105 мм, и частоте обхода 1,43 ГГц. Ненулевые значения расстройки Δ_k введены для моделирования спектральной неоднородности массива. Фазовый набег сигнала обратной связи для простоты принят равным нулю. Пороговое значение нормированного параметра накачки вычисляется как

$$J_{thr} = ((1+g)(B(g-1)+g)) / (gB(g-1)). \quad (5)$$

Моделирование динамики массива, состоящего из трех связанных лазеров на основе МкС с КТ с оптической обратной связью, было

Таблица 1. Принятые значения параметров модели

Параметр	Значение
Количество связанных лазеров в массиве	3
Дифференциальное усиление	1,15
Фактор уширения линии	2
Время жизни фотона, пс	7
Время релаксации заселенности точки, нс	0,1
Время релаксации смачивающего слоя, нс	0,1
Скорость захвата носителей заряда	924
Значение расстройки между частотой первого лазера массива и опорной частотой, ГГц	–4
Значение расстройки между частотой второго лазера массива и опорной частотой, ГГц	0
Значение расстройки между частотой третьего лазера массива и опорной частотой, ГГц	4
Фазовый набег $\varphi_1 = \varphi_2 = \varphi_3$	0
Нормированный параметр накачки	$1{,}5J_{thr}$

осуществлено посредством численного интегрирования представленной системы дифференциальных уравнений с использованием полуимплицитного метода Эйлера, реализованного на языке Julia.

БИФУРКАЦИОННЫЙ АНАЛИЗ МОДЕЛИ МАССИВА СВЯЗАННЫХ ЛАЗЕРОВ НА ОСНОВЕ МИКРОСТОЛБИКОВ С КВАНТОВЫМИ ТОЧКАМИ С ОПТИЧЕСКОЙ ОБРАТНОЙ СВЯЗЬЮ

На рис. 2 представлены бифуркационные диаграммы, полученные при изменении параметра силы обратной связи γ. Как следует из данных диаграмм, при значениях $\gamma < 0{,}03$ система демонстрирует периодический и квазипериодический режимы лазерной генерации. Изначально в сигнале суммарной интенсивности наблюдаются частоты, связанные с расстройкой частоты отдельных лазеров. При увеличении силы обратной связи происходит расщепление данных частот вследствие появления мод внешнего резонатора и эффекта четырехволнового взаимодействия, определяемого в модели фактором уширения линии α.

Увеличение силы обратной связи приводит к появлению все большего числа мод внешнего резонатора и в результате их взаимодействия — к хаотическому режиму генерации при $\gamma > 0{,}03$. В интенсивности при этом наблюдается след времени запаздывания обратной связи, проявляющийся в виде пиков радиочастотного спектра на частоте обхода резонатора

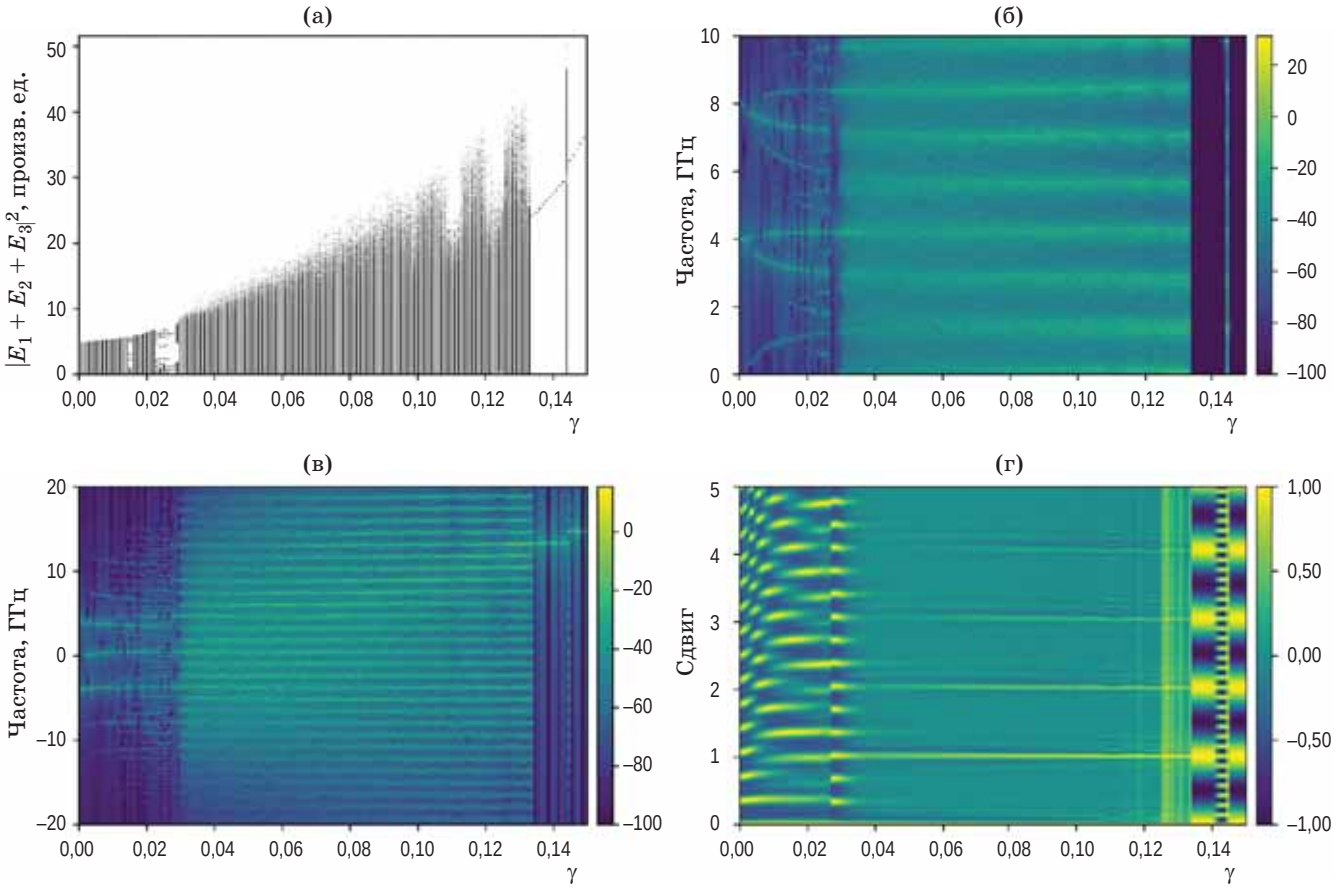

Рис. 2. Результаты моделирования динамики массива лазеров на основе МкС с КТ. Бифуркационная диаграмма (а), показывающая экстремумы интенсивности суммарного поля лазерного излучения массива лазеров на основе микростолбиков с квантовыми точками с внешней обратной оптической связью при изменении параметра силы обратной связи γ. Соответствующие радиочастотный (б) и оптический (в) спектры суммарного поля $E_1+E_2+E_3$, цветные шкалы соответствуют спектральной плотности мощности в децибелах. Автокорреляционная функция интенсивности суммарного поля (г), вертикальная ось соответствует сдвигу, выраженному во времени запаздывания внешней оптической обратной связи

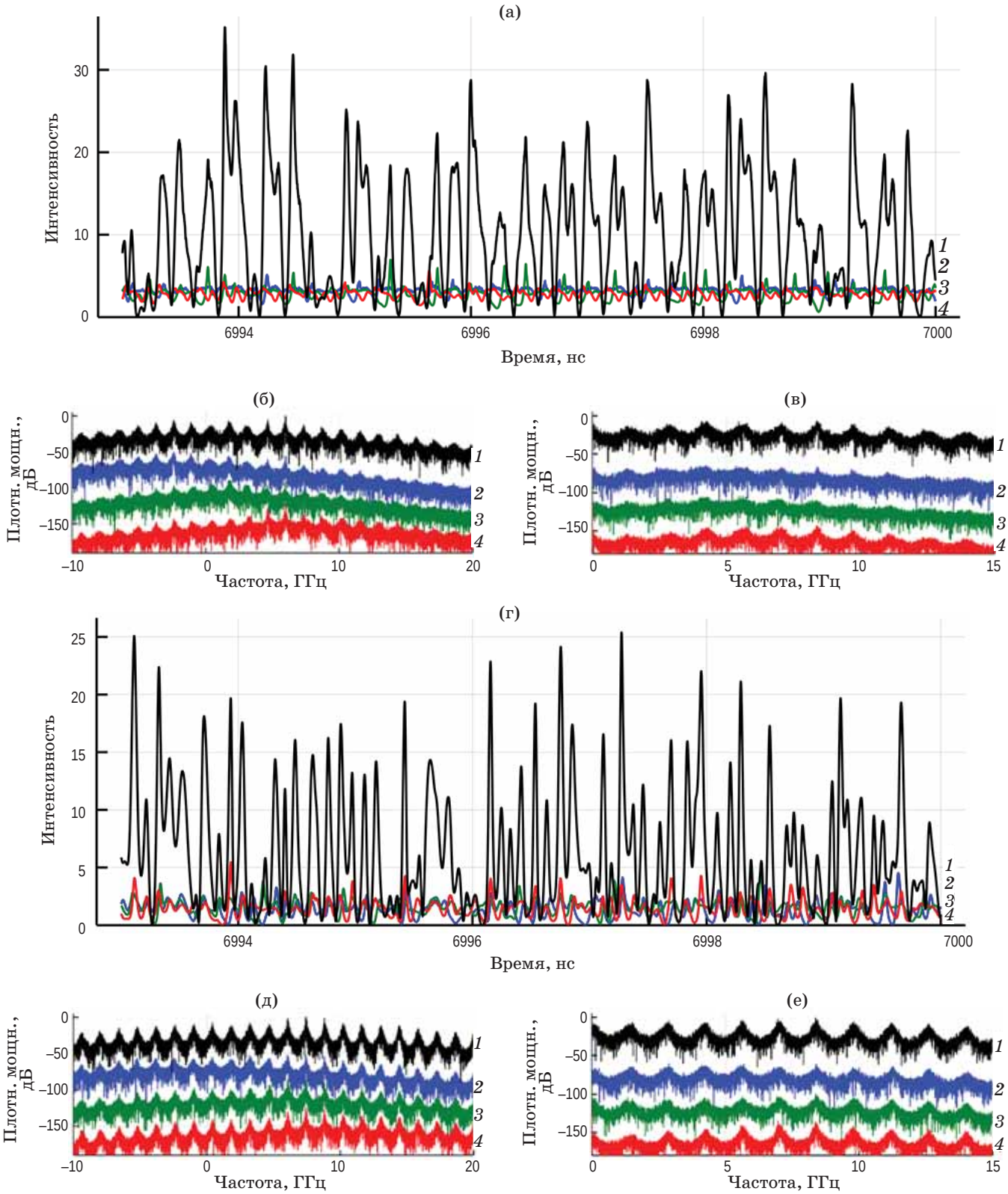

Рис. 3. Результаты моделирования динамики массива лазеров на основе МкС с КТ и отдельных лазеров на основе МкС с КТ при $\gamma = 0{,}045$ (а, б, в), $\gamma = 0{,}08$ (г, д, е). Временные диаграммы (а, г), оптические (б, д) и радиочастотные (в, е) спектры излучения лазеров на основе МкС с КТ. *1* — результаты расчета для массива лазеров на основе МкС с КТ, *2*, *3*, *4* — результаты расчета для отдельных лазеров из массива. На изображениях оптических и радиочастотных спектров для наглядности спектры для отдельных лазеров массива сдвинуты вниз на 40, 80 и 120 дБ соответственно

и ее гармониках (рис. 1б), а также в виде пиков корреляционной функции (рис. 1г) при временах сдвига, кратных времени запаздывания. Подобного рода эффект потенциально может оказывать негативное влияние на генерацию случайных чисел. При $\gamma > 0{,}132$ система входит в режим синхронизации, и весь массив осуществляет генерацию на единственной частоте внешнего резонатора. В процессе дальнейшего увеличения силы обратной связи в области $\gamma = 0{,}145$ система претерпевает перескок моды генерации на соседнюю по частоте моду.

На рис. 3 приведены примеры временных диаграмм, оптических и радиочастотных спектров при значениях силы обратной связи $\gamma = 0{,}045$ (а, б, в) и $\gamma = 0{,}08$ (г, д, е). Как видно, система демонстрирует хаотическую генерацию, при этом в спектре сигнала присутствуют гармоники, соответствующие частоте обхода обратной связи.

ГЕНЕРАЦИЯ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СЛУЧАЙНЫХ БИТОВ

Для моделирования битовой последовательности, являющейся результатом работы генератора случайных чисел с использованием массива связанных лазеров на основе МкС с КТ с оптической обратной связью, использовался алгоритм, схожий с описанным ранее в публикации [14].

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 12 бит, что соответствует 4096 уровням),

3) дискретизированные значения интенсивности из диапазона от 0 до 4095 переводятся в битовое представление,

4) для каждого битового представления выбираются четыре младших разряда,

5) осуществляется конкатенация полученных битовых значений в итоговую битовую последовательность.

Была осуществлена проверка случайности последовательностей длиной 11142860 битов, полученных на основе данного алгоритма, для параметров, соответствующих рис. 3, с частотой 100 гигавыборок в секунду. На заключительном этапе выполнена проверка случайности сгенерированных последовательностей с использованием статистических

Таблица 2. Результаты проверки битовой последовательности на случайность согласно статистическим тестам NIST 800-22

Тест	p-значение	
	$\gamma = 0{,}045$	$\gamma = 0{,}08$
Частотный побитовый тест	0,339	0,329
Частотный блочный тест	0,932	0,670
Тест серий	0,048	0,640
Тест на длиннейшую серию единиц в блоке	0,798	0,334
Тест рангов бинарных матриц	0,116	0,909
Спектральный тест на основе дискретного преобразования Фурье	0,414	0,790
Тест на совпадение неперекрывающихся шаблонов	0,192	0,912
Тест на совпадение перекрывающихся шаблонов	0,216	0,841
Универсальный тест Маурера	0,708	0,813
Тест на линейную сложность	0,687	0,728
Тест на периодичность	0,696	0,333
	0,720	0,407
Тест приблизительной энтропии	0,973	0,667
Тест кумулятивных сумм (прямой)	0,224	0,314
Тест кумулятивных сумм (обратный)	0,661	0,505

тестов NIST 800-22 [4], реализованных на языке Python [17]. Результаты проверки приведены в табл. 2.

Проверка считается пройденной успешно в том случае, если p-значение превышает 0,01. Из табл. 2 видно, что условие успешного прохождения статистических тестов выполнено для всех исследованных последовательностей, соответствующих хаотическому режиму генерации массива связанных лазеров на основе МкС с КТ с оптической обратной связью. При этом не выявлено негативное влияние следа времени запаздывания обратной связи на результаты прохождения теста.

ЗАКЛЮЧЕНИЕ

Представлена математическая модель массива связанных лазеров на основе МкС с КТ с оптической обратной связью, проведен ее бифуркационный анализ. Показано, что воздействие обратной оптической связи приводит к хаотической генерации массива связанных лазеров на основе МкС с КТ, что может быть использовано для генерации последовательностей случайных битов. Приведены результаты моделирования процесса генерации последовательностей случайных битов со скоростью 400 Гбит/с, успешно прошедших 14 статистических тестов NIST 800-22 для p-значения, равного 0,01.

СПИСОК ИСТОЧНИКОВ

1. Hirano K., Yamazaki T., Morikatsu S., Okumura H., Aida H., Uchida A., Yoshimori S., Yoshimura K., Harayama T., Davis P. Fast random bit generation with bandwidth-enhanced chaos in semiconductor lasers // Opt. Exp. 2010. V. 18. № 6. P. 5512–5524. https://doi.org/10.1364/OE.18.005512
2. Li N., Kim B., Choi D., Chizhevsky V.N., Locquet A., Bloch M., Citrin D.S., Pan W. Fast random bit generation with a single chaotic laser subjected to optical feedback // Semiconductor Lasers and Laser Dynamics VI. Belgium, 2 May 2014. P. 9134271–9134276.
3. Kim G., In J.H., Kim Y.S., Rhee H., Park W., Song H., Park J., Kim K.M. Self-clocking fast and variation tolerant true random number generator based on a stochastic mott memristor // Nature Commun. 2021. V. 12. № 1. P. 1–8.
4. Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S., Levenson M., Vangel M., Banks D., Heckert A., Dray J. Statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST, 2010.
5. 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 // Opt. Lett. 2016. V. 41. № 2. P. 388–391.
6. Sciamanna M., Shore K.A. Physics and applications of laser diode chaos // Nature Photonics. 2015. V. 9. № 3. P. 151–162.
7. Oliver N., Soriano M.C., Sukow D.W., Fischer I. Fast random bit generation using a chaotic laser: Approaching the information theoretic limit // IEEE J. Quantum Electron. 2013. V. 49. № 11. P. 910–918.
8. 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. № 1. P. 1–8.
9. 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 // Opt. Exp. 2012. V. 20. № 27. P. 28603–28613.
10. Virte M., Mercier E., Thienpont H., Panajotov K., Sciamanna M. Physical random bit generation from chaotic solitary laser diode // Opt. Exp. 2014. V. 22. № 14. P. 17271–17280.
11. Rontani D., Locquet A., Sciamanna M., Citrin D.S. Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback // Opt. Lett. 2007. V. 32. № 20. P. 2960–2962.
12. 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 Commun. 2019. V. 10. № 1. P. 1–11.
13. Gies C., Reitzenstein S. Quantum dot micropillar lasers // Semiconductor Sci. and Technol. 2019. V. 34. № 7. P. 073001.
14. Petrenko A.A., Kovalev A.V., Bougrov V.E. Random number generation with arrays of coupled micropillar quantum dot lasers // Scientific and Technical J. Information Technologies, Mechanics and Optics. 2021. V. 21. № 6. P. 962–968.

15. Kozyreff G., Vladimirov A.G., Mandel P. Global coupling with time delay in an array of semiconductor lasers // Phys. Rev. Lett. 2000. V. 85. № 18. P. 3809–3812.
16. 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. № 1. P. 1–8.
17. Kho Ang S. NIST Randomness Testsuit [Электронный ресурс]. Режим доступа: https://github.com/stevenang/randomness_testsuite, свободный. Яз. англ. (дата обращения: 25.05.2022).

АВТОРЫ

Артем Александрович Петренко — ассистент ИПСПД, Университет ИТМО, Санкт-Петербург, 197101, Россия; Scopus ID 57210121963; https://orcid.org/0000-0002-7862-971X; aapetrenko@itmo.ru

Антон Владимирович Ковалев — кандидат физико-математических наук, доцент ИПСПД, Университет ИТМО, Санкт-Петербург, 197101, Россия; Scopus ID 56205289400; https://orcid.org/0000-0001-7848-8526; avkovalev@itmo.ru

Владислав Евгеньевич Бугров — доктор физико-математических наук, профессор, директор ИПСПД, Университет ИТМО, Санкт-Петербург, 197101, Россия; Scopus ID 8321276100; https://orcid.org/0000-0002-5380-645X; vladislav.bougrov@itmo.ru

AUTHORS

Artem A. Petrenko — Assistant, ITMO University, St. Petersburg, 197101, Russian Federation; Scopus ID 57210121963; https://orcid.org/0000-0002-7862-971X; aapetrenko@itmo.ru

Anton V. Kovalev — Candidate of Physico-Mathematical Sciences, Associate Professor, ITMO University, St. Petersburg, 197101, Russian Federation; Scopus ID 56205289400; https://orcid.org/0000-0001-7848-8526; avkovalev@itmo.ru

Vladislav E. Bougrov — Doctor of Physico-Mathematical Sciences, Full Professor, Director Institute of Advanced Data Transfer Systems, ITMO University, St. Petersburg, 197101, Russian Federation; Scopus ID 8321276100; https://orcid.org/0000-0002-5380-645X; vladislav.bougrov@itmo.ru

Статья поступила в редакцию 30.05.2022, одобрена после рецензирования 15.06.2022, принята к печати 11.07.2022