

09;07.3

Генерация случайных последовательностей за счет переключения поперечных мод в квантовом каскадном лазере

© В.В. Дюделев¹, Е.Д. Черотченко¹, Д.А. Михайлов¹, Д.В. Чистяков¹, С.О. Слипченко¹, А.В. Лютецкий¹, А.Г. Гладышев², А.В. Бабичев¹, Л.Я. Карачинский², И.И. Новиков², Н.А. Пихтин¹, А.Ю. Егоров³, А.В. Кондрашов⁴, А.А. Семенов⁴, Г.С. Соколовский¹, А.Б. Устинов⁴

¹ Физико-технический институт им. А.Ф. Иоффе РАН, Санкт-Петербург, Россия

² ООО „Коннектор Оптикс“, Санкт-Петербург, Россия

³ Санкт-Петербургский национальный исследовательский Академический университет им. Ж.И. Алфёрова РАН, Санкт-Петербург, Россия

⁴ Санкт-Петербургский государственный электротехнический университет „ЛЭТИ“, Санкт-Петербург, Россия

E-mail: ustinov-rus@mail.ru

Поступило в Редакцию 15 сентября 2023 г.

В окончательной редакции 2 октября 2023 г.

Принято к публикации 2 октября 2023 г.

Исследована генерация случайных битовых последовательностей за счет переключения поперечных мод в квантово-каскадном лазере (ККЛ). Для приема излучения использовался квантово-каскадный детектор (ККД), изготовленный из гетероструктуры ККЛ, что открывает возможность их объединения в фотонной интегральной схеме. Исследование проведено для длительности импульсов накачки ККЛ 130 пс с частотой повторения 10–100 кГц. Показано, что на выходе оптопары ККЛ–ККД возникают электрические импульсы со случайно меняющейся величиной напряжения, которые при соответствующем компарировании преобразуются в случайные битовые последовательности.

Ключевые слова: интегральная оптика, квантово-каскадный лазер, генератор случайных чисел.

DOI: 10.61011/PJTF.2023.22.56598.19729

Случайные последовательности чисел или битов в настоящее время находят различные приложения в науке и технике. Так, например, их используют для моделирования стохастических систем, а также для генерации криптографических ключей. В основе работы генераторов случайных чисел (ГСЧ), реализуемых аппаратными способами, лежат те или иные физические процессы. Ими могут быть хаотические или шумовые процессы, а также неустойчивости различных видов, возникающие в нелинейных динамических системах. Классическими примерами таких процессов могут служить тепловой шум резистора, дробовый шум в полупроводниковых стабилитронах или вакуумных лампах, радиоактивный распад в радиоактивных материалах, неустойчивость частоты генерации осцилляторов [1–4].

В работе [5] было показано, что квантовые каскадные лазеры (ККЛ) являются перспективными источниками для создания ГСЧ для защищенных систем беспроводной оптической связи. Описанные подходы позволяют получить устойчивый режим генерации случайных битовых последовательностей, однако применение внешнего резонатора и фотоприемников на основе твердых растворов кадмий–ртуть–теллур не позволяет создавать компактные и устойчивые к вибрациям интегрально-оптические устройства. Более перспективным подходом для генерации случайных последовательностей является регистрация пространственно-временных неоднородностей интенсивности выходного излучения вследствие многомодовой генерации полупроводниковых лазеров с

широким полоском [6]. Последние исследования в области создания квантово-каскадных детекторов (ККД) [7] открывают широкие возможности для создания компактных интегрально-оптических устройств на основе оптопар ККЛ–ККД.

В настоящей работе проведены исследования по созданию ГСЧ на основе пары ККЛ–ККД. ККЛ и ККД изготавливались из одной и той же гетероструктуры с активной областью на основе гетеропары InGaAs/InAlAs, изопериодичной с подложкой InP, с помощью двухстадийного эпитаксиального роста. Активная область изготавливалась методом молекулярно-пучковой эпитаксии (ООО „Коннектор Оптикс“). Верхняя волноводная обкладка InP и контактный слой InGaAs выращивались методом газофазной эпитаксии из металлоорганических соединений (АО „НИИ „Полус“ им. М.Ф. Стельмаха“). Подробное описание структуры приведено в работе [8].

Постростовая обработка гетероструктур включала в себя последовательно следующие операции: нанесение фоторезистивной маски и травление через нее канавок, формирующих гребневый волновод, нанесение диэлектрика, вскрытие контактных окон и напыление верхнего и нижнего контактов. Готовая пластина раскальвалась на чипы и монтировалась на первичный медный теплоотвод эпитаксиальным слоем вниз. Используемые в исследовании ККЛ имели ширину полоска 60 μm и длину резонатора 4.5 mm. Процедура постростовой обработки ККД была идентична таковой для ККЛ. Монтаж ККД на первичный теплоотвод эпитаксиальным слоем вниз

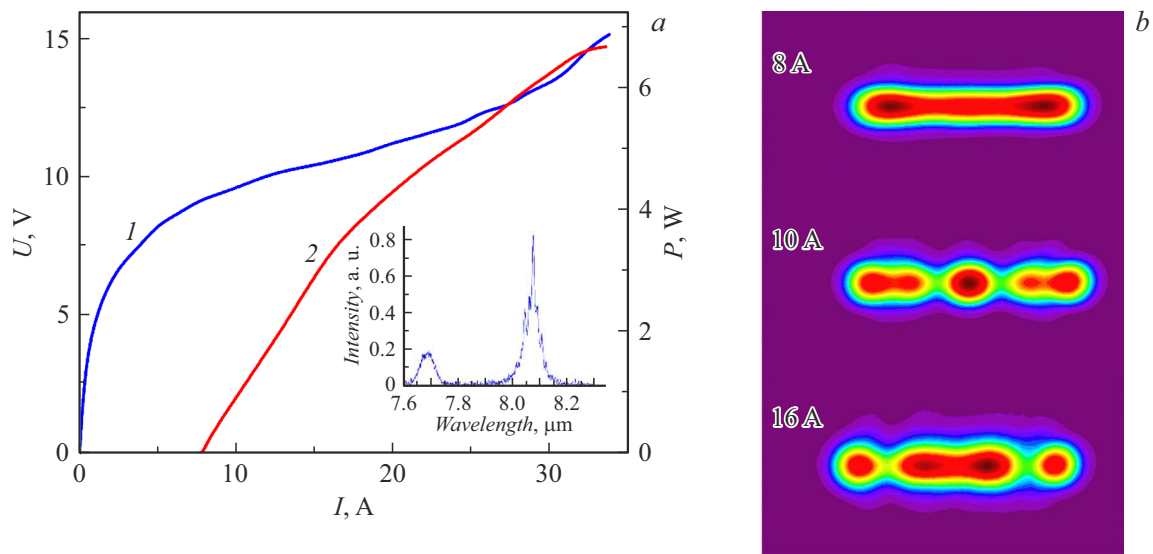


Рис. 1. *a* — типичные вольт-амперная (1) и ватт-амперная (2) характеристики ККЛ. Приведена мощность с одного зеркала. На вставке представлен типичный спектр генерации ККЛ при токе накачки 15 А. *b* — распределение интенсивности ККЛ в ближнем поле для токов 8, 10 и 16 А. Накачка ККЛ осуществлялась импульсами тока амплитудой с длительностью ~ 130 ns при частоте повторения 11.5 kHz.

осуществлялся аналогично ККЛ. Длина чипов ККД и ширина полосков составляли ~ 0.5 mm и 10 μ m соответственно. Таким образом, соотношение между ширинами принимающей и излучающей апертур составляло 1/6. Такое соотношение ширин полосков ККД/ККЛ позволяло детектировать излучение лишь небольшой части выходного зеркала ККЛ, обеспечивая тем самым регистрацию пространственно-временной неоднородности интенсивности ККЛ, возникающей вследствие многомодовой генерации.

Выходные характеристики ККЛ были исследованы в импульсном режиме. Длительность импульса накачки составляла ~ 130 ns при частоте повторения 11.5 kHz. Типичные вольт-амперная и ватт-амперная характеристики ККЛ представлены на рис. 1, *a*. Выходная мощность приведена для излучения с одного зеркала. Типичный спектр генерации показан на вставке к рис. 1, *a*. Максимум спектра генерации (вставка к рис. 1, *a*) соответствует 8.1 μ m, что отвечает окну прозрачности атмосферы.

Были проведены исследования пространственных характеристик выходного излучения ККЛ, результаты которых представлены на рис. 1, *b*. Исследования проводились при помощи болометрической камеры Dataray IR-BB. Схема исследования пространственных характеристик ККЛ подробно описана в работе [9]. Поскольку быстродействие камеры составляет 8 Hz, представленная картина распределения интенсивности в ближнем поле ККЛ является усредненной. Хорошо видно, что по мере увеличения амплитуды тока накачки происходит увеличение количества поперечных мод, участвующих в генерации. При повышении тока накачки выше 14 А картина ближнего поля визуально не меняется, что указывает на генерацию на максимально возможном

количестве поперечных мод. Исходя из исследования ватт-амперной характеристики ККЛ для реализации ГСЧ был выбран рабочий ток 16 А. При этом токе не наступает насыщения ватт-амперной характеристики, но наблюдается устойчивая генерация на максимальном количестве латеральных мод, что обеспечивает необходимую пространственно-временную неоднородность интенсивности излучения ККЛ. Дальнейшее повышение рабочего тока не имело практического смысла, так как детектирование сигнала было уверенным и наблюдалась устойчивая генерация случайных последовательностей.

Схема установки для реализации ГСЧ на основе оптопары ККЛ–ККД представлена на рис. 2, *a*. Излучение ККЛ фокусировалось на входную апертуру фотоприемника при помощи оптической системы с коэффициентом увеличения 1. Все элементы оптической системы, ККЛ и ККД устанавливались на высокоточные трехкоординатные микропозиционеры с нанометровой чувствительностью, что обеспечивало эффективный ввод излучения в волновод ККД. Излучение (и поглощение), связанное с внутризонными переходами в квантовых ямах и структурах на их основе, в том числе ККЛ и ККД, имеет ТМ-поляризацию. Поэтому накачка ККД осуществлялась в торец, чтобы обеспечить необходимую поляризацию излучения.

Как было показано в работе [6], наличие генерации на множестве латеральных мод приводит к хаотической зависимости распределения интенсивности излучения по зеркалу лазера от времени. Поэтому для получения ГСЧ необходимо обеспечивать пространственную селективность схемы детектирования. В построенной оптической схеме соотношение апертур ККД и ККЛ было 1/6, что обеспечивало необходимое пространственное

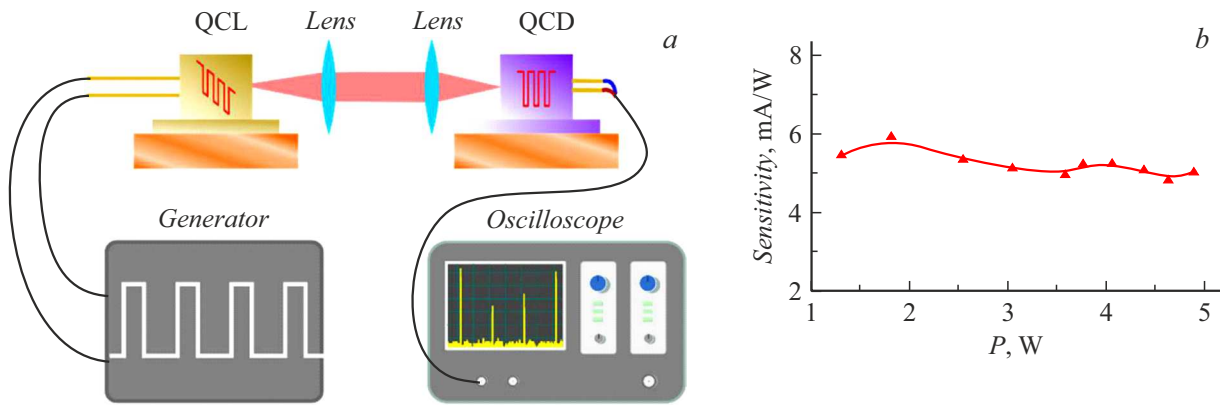


Рис. 2. *a* — блок-схема ГСЧ на основе пары ККЛ–ККД; *b* — зависимость чувствительности ККД от мощности накачки при реализации ГСЧ.

разрешение для регистрации флуктуаций интенсивности излучения конкурирующих мод. Токовая накачка ККЛ осуществлялась при помощи генератора импульсов тока. ККЛ охлаждался при помощи термоэлектрического охладителя с водяным охлаждением. ККД подключался к осциллографу при помощи коаксиального кабеля с волновым сопротивлением 50Ω . Для регистрации излучения ККД не требуется смещения, что схематически показано на рис. 2, *a*. Исследования чувствительности ККД показали, что она остается постоянной во всем диапазоне токов накачки и составляет ~ 12 и 5.5 mA/W при накачке ККЛ с шириной полоска 16 и $60 \mu\text{m}$ соответственно (рис. 2, *b*). Верхний предел мощности детектируемого излучения ККД определялся максимальной выходной мощностью имеющихся в нашем распоряжении ККЛ. Снижение чувствительности при увеличении ширины полоска ККЛ связано с увеличением размера фокусного пятна по сравнению с входной апертурой, что обеспечивает необходимое пространственное разрешение схемы регистрации, но снижает эффективность ввода излучения в ККД.

При проведении исследований устанавливалась длительность импульсов токовой накачки $\tau = 130 \text{ ns}$. Период импульсов T варьировался от 10 до $100 \mu\text{s}$, что соответствовало частоте следования импульсов $f = 10\text{--}100 \text{ kHz}$. При этом верхний предел частоты следования импульсов определялся исключительно возможностями драйвера управления ККЛ. Измерения последовательностей импульсов проводились с помощью осциллографа реального времени Tektronix DPO 7354. Частота дискретизации была установлена 100 Ms/s (10 ns/pt), что соответствовало 13 точкам на импульс. Длительность измеренных осциллограмм составляла 200 ms . Таким образом, количество измеренных импульсов в каждой осциллограмме составляло от 2000 до $20\,000$ в зависимости от периода.

Типичная осциллограмма напряжения на выходе ГСЧ показана на рис. 3. Видно, что импульсы напряжения меняют свою величину случайным образом в диапазоне

$0.18\text{--}0.4 \text{ V}$. Экспериментально измеренное напряжение импульсов варьировалось в некотором диапазоне между минимальным и максимальным значениями. Далее последовательность импульсов компарировалась. Пороговое напряжение компаратора U_i выбиралось между минимальным и максимальным значениями напряжения импульсов.

Для проверки случайности полученных битовых последовательностей использовались пять тестов из набора статистических тестов NIST [10]. В частности, были использованы частотный побитовый тест (Frequency (Monobit) Test), частотный блочный тест (Frequency Test within a Block), тест на последовательность одинаковых битов (Runs Test), тест на самую длинную последовательность единиц в блоке (Test for the Longest Run of Ones in a Block) и спектральный тест (Discrete Fourier Transform (Spectral) Test). Первый тест определяет, чего в последовательностях больше (нулей или единиц). Тест считается пройденным, если единиц примерно столько же, сколько нулей. Второй тест аналогичен первому, но проверяет отдельные блоки исходной последователь-

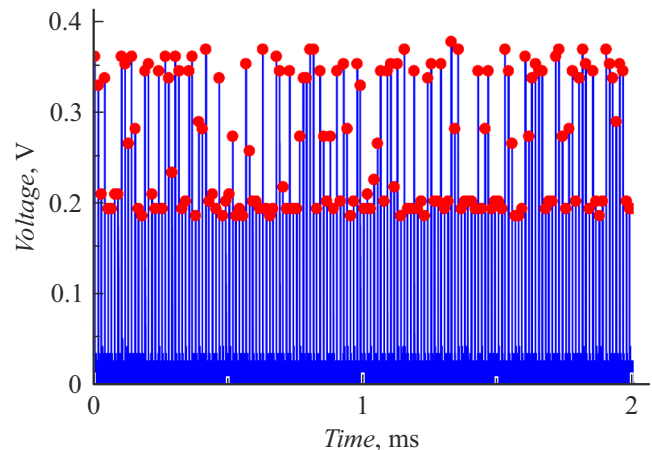


Рис. 3. Типичный фрагмент осциллограммы для периода импульсов токовой накачки $T = 16.7 \mu\text{s}$.

ности. Третий тест оценивает количество и длины блоков, состоящих из одинаковых битов в исследуемой последовательности, и соответствие этой длины абсолютно случайной последовательности. Как следует из названия, при проведении четвертого теста определялась максимальная длина блока, состоящего только из единиц, и то, насколько она характерна случайной последовательности. В ходе последнего теста с помощью дискретного преобразования Фурье оценивалось, есть ли в спектре максимумы, свидетельствующие о наличии в битовой последовательности периодически повторяющихся участков. Для каждого теста рассчитывалась величина p , называемая вероятностью. Если значение p было больше 0.01, то тест считался пройденным. Те последовательности, которые успешно проходили все выбранные тесты, считались случайными.

Результаты обработки временных реализаций и тестирования полученных последовательностей показали, что для приведенной импульсной последовательности напряжение компарации U_t , при котором последовательность битов оказывается случайной, лежит в диапазоне от 250 до 300 мВ.

Проведенное исследование показывает, что широкополосковые ККЛ, генерирующие множество латеральных мод, подобно лазерным диодам [6], демонстрируют пространственно-временную неоднородность распределения интенсивности излучения на выходном зеркале, связанную с конкуренцией мод. Поэтому предложенная конструкция генератора на основе оптопары ККЛ–ККД позволяет уверенно формировать случайные битовые последовательности. При этом наиболее предпочтительным является режим генерации электрических импульсов с разбросом напряжения между минимальным и максимальным значениями. Для увеличения частоты генерации представляется возможным использовать линейку ККД, объединенных с широкополосковым ККЛ в единой фотонной интегральной схеме. Предварительные оценки указывают на возможность увеличения таким образом частоты генерации до десятков-сотен мегагерц.

Финансирование работы

В части изготовления оптопары ККЛ–ККД исследование выполнено в рамках научной программы Национального центра физики и математики (проект „Физика высоких плотностей энергии. Этап 2023–2025“). В части проведения экспериментов по генерации случайных битовых последовательностей и анализа данных исследование выполнено при поддержке проекта СПбГЭТУ „ЛЭТИ“ программы стратегического академического лидерства „Приоритет-2030“.

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

- [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. Varanono, *IEEE Trans. Comput.*, **52** (4), 403 (2003). DOI: 10.1109/TC.2003.1190581
- [3] А.Б. Устинов, А.В. Кондрашов, Б.А. Калинин, *Письма в ЖТФ*, **42** (8), 28 (2016). [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/acsp Photonics.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] В.В. Дюделев, Д.А. Михайлов, В.Ю. Мыльников, А.В. Бабишев, С.Н. Лосев, Е.А. Когновицкая, А.Г. Гладышев, Л.Я. Карачинский, И.И. Новиков, Д.В. Денисов, С.О. Слипченко, А.В. Лютецкий, Н.А. Пихтин, В.И. Кучинский, А.Ю. Егоров, Г.С. Соколовский, *Письма в ЖТФ*, **46** (22), 51 (2020). DOI: 10.21883/PJTF.2020.22.50310.18501 [V.V. Dudelev, D.A. Mikhailov, V.Yu. Myl'nikov, A.V. Babichev, S.N. Losev, E.A. Kognovitskaya, A.G. Gladyshev, L.Ya. Karachinsky, I.I. Novikov, D.V. Denisov, 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