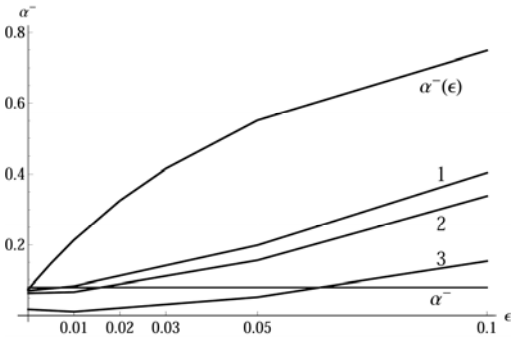


# БЫСТРОДЕЙСТВУЮЩАЯ ГЕНЕРАЦИЯ СЛУЧАЙНЫХ БИТ НА ОСНОВЕ СТОХАСТИЧЕСКИХ ПРОЦЕССОВ В ПОЛУПРОВОДНИКОВОМ ВЕРТИКАЛЬНО-ИЗЛУЧАЮЩЕМ ЛАЗЕРЕ

**В. Н. Чижевский**

*Институт физики имени Б. И. Степанова*
*Минск, Беларусь*
*E-mail: vnc@dragon.bas-net.by*

Экспериментально продемонстрировано, что поляризационный шум в полупроводниковом лазере с вертикальным резонатором является эффективным источником энтропии для быстрой генерации случайных бит. В зависимости от метода извлечения случайных бит, эффективная скорость генерации может составлять от 100 Мбит/с до 4,5 Гбит/с при частоте дискретизации 100 МГц. Генерируемые последовательности случайных бит характеризуются низким смещением, отсутствием корреляций между битами и проходят основные статистические тесты на случайность.

*Ключевые слова*: полупроводниковый вертикально-излучающий лазер, поляризационный шум, генерация случайных бит.

Генерация случайных чисел имеет первостепенное значение для криптографии, моделирования Монте-Карло и программирования, численного анализа, а также для ряда коммерческих применений. Один из способов получения случайных чисел состоит в использовании числовых процедур (так называемые «генераторы псевдослучайных числовых последовательностей»). Они производят множество чисел, имеющих близкое подобие последовательностям истинных случайных чисел [1]. Другой подход к генерации случайных чисел основан на использовании недетерминированных физических процессов с внутренне присущей случайностью. Среди них можно отметить физические процессы типа радиоактивности [2], шум резисторов или полупроводниковых диодов [3], оптические квантовые процессы, такие как отражение фотонов на 50/50 светоделителе [4], или шумы спонтанной эмиссии светоизлучающих диодов [5]. В последнее время большое внимание было уделено исследованиям, направленным на получение быстрой генерации случайных бит в гигагерцовом диапазоне на основе использования хаотической динамики в полупроводниковых лазерах с оптической обратной связью [6–8].

В данной работе представлены результаты, демонстрирующие возможность быстрой генерации случайных бит на основе использования поляризационных шумов в полупроводниковом лазере с вертикальным резонатором в качестве источника энтропии. Подобные лазеры широко применяются в коммуникационных системах, обладают невысокой стоимостью изготовления и компактностью. Ранее было показано, что спонтанные переключения в области поляризационной бистабильности в лазерах с вертикальным резонатором могут быть использованы для генерации случайных бит со скоростью порядка 300 кбит/с [9]. В данной работе предлагается использовать другой режим поляризационных неустойчивостей, которые могут наблюдаться при больших токах накачки, значительно выше порога генерации. В частности, в работе [10] было отмечено, что в этих условиях наблюдаются достаточно быстрые (в субнаносекундном временном диапазоне) флуктуации интенсивности лазера на выделенной поляризации, распределение амплитуд которых близко к нормальному закону. Именно этот режим используется здесь для быстрой генерации случайных чисел. Кроме того, для увеличения скорости генерации применяется также разработанный недавно метод извлечения случайных бит из экспериментальных данных, который позволяет увеличить скорость генерации бит в 45 раз по отношению к средней частоте случайных событий или частоте дискретизации случайного аналогового процесса [11]. Использование этого подхода позволило получить эффективную частоту генерации случайных бит 4,5 Гбит/с при частоте дискретизации сигналов 100 МГц.

Исследования были выполнены на экспериментальной установке, аналогичной использованной ранее для генерации случайных бит [9, 11]. Использовался полупроводниковый вертикально-излучающий лазер, генерирующий в области 850 нм. Лазер был термостабилизирован с точностью до 0.005 °C. Величина тока накачки программно управлялась от компьютера. Интенсивность лазера на выделенной поляризации регистрировалась быстродействующим фотодиодом и оцифровывалась с помощью USB цифрового осциллографа с выборочным периодом $t_s$ =10 нс и разрешением 8-бит. В результате на выходе получалась последовательность случайных 8-битовых целых чисел $\{a_k\}$ ($k$ = 1, 2, … ).

Прежде всего были исследованы статистические характеристики поляризационных шумов в широком диапазоне токов накачки. Целью эти исследований было на-

хождение условий, при которых амплитуда флуктуаций максимальна, а функция распределения поляризационных шумов наиболее симметрична. В работе [11] было отмечено, что высокая симметрия распределения случайных данных является необходимым условием для получения равномерно распределенных случайных бит. В эксперименте напряжение, приложенное к лазерному диоду, дискретно менялось от 1 В до 3 В с шагом 0,5 мВ. При этом определялись следующие статистические характеристики: среднее значение флуктуаций μ, стандартное отклонение σ, коэффициент асимметрии $S = \mu_3/\sigma^3$ и коэффициент эксцесса $K = \mu_4/\sigma^4$ , где $\mu_3$ и $\mu_4$ – соответственно третий и четвертый центральные моменты распределения поляризационного шума. Было найдено, что в области напряжений примерно 2,9 В амплитуда флуктуаций становится достаточно большой, для того чтобы использовать в качестве источника шума для генерации случайных чисел. При определенном значении напряжения на диоде поляризационный шум хорошо описывается нормальным законом распределения. На рисунке 1, *а* представлены зависимости коэффициента асимметрии $S$ и коэффициента эксцесса $K$ от величины приложенного напряжения, нормированного на значение порога генерации. В частности, видно, что $S \approx 0$, в то время как $K \approx 3$, что соответствует нормальному закону распределения. При фиксированном значении тока накачки симметрия распределения может также достаточно хорошо контролироваться с помощью поворота полуволновой пластинки (рис. 1, *б*). В дальнейшем, во всех экспериментах по генерации случайных бит, величина приложенного напряжения и угол поворота полуволновой пластинки были выбраны таким образом, чтобы $S \approx 0$ и $K \approx 3$. Пример временного поведения интенсивности лазера на выделенной поляризации, демонстрирующие быстрые случайные флуктуации, индуцированные шумами спонтанной эмиссии, представлен на рис. 2, *а*. На рисунке 2, *б* показана функция плотности вероятности распределения амплитуд $\{a_k\}$.

Вначале для оценки качества произведенных случайных бит использовались две индикатора, а именно, статистическое смещение, определяемое как $B = < b_i > - 0.5$, где $<b_i>$ – среднее значение по анализируемой последовательности случайных бит $\{b_i\}$ и сериальные коэффициенты автокорреляции, определяемые как

$C_k = \left\langle \left(b_i - \langle b_i \rangle\right)\left(b_{i+k} - \langle b_i \rangle\right)\right\rangle \Big/ \left\langle \left(b_i - \langle b_i \rangle\right)^2 \right\rangle$, где $k$ – задержка в битах, $\langle ... \rangle$ – усреднение производится по индексу $i$. Статистическое смещение $B$ и коэффициенты автокорреляции $C_k$ являются случайными переменными, которые меняются от одной последовательности к другой и зависят от ее длины $N$ [1]. В этом случае стандартное отклонение $\sigma_B$ для статистического смещения от величины 0.5 и стандартное отклонение $\sigma_C$ для коэффициентов автокорреляции определяются соответственно следующими выражениями: $\sigma_B = 0.5\, N^{-0.5}$ и $\sigma_C = N^{-0.5}$ [1].

Рассмотрим наиболее простой метод извлечения случайных бит. Экспериментально измеренные последовательности $\{a_k\}$ преобразовывались в последовательность бит по следующему правилу: каждое значение амплитуды шума $\{a_k\}$ отображалось в бинарное представление $b_7..b_1b_0$, где $b_m$ $(m = 0,1,...7)$ принимает два значения «0» или «1». Далее, извлекались последовательности $\{b_{m,i}\}$ $(i = 1,2,...)$. При этом для каждой последовательности анализировалось статистическое смещение $B$ и коэффициенты автокорреляция $C_k$. В частности, было найдено, что наилучшие в статистическом смысле результаты получаются для последовательности $\{b_{4,i}\}$. На рисунке 3, *а* в двойном логарифмическом масштабе показано поведение статистического смещения $B$ в зависимости от длины генерируемой последовательности $\{b_{4,i}\}$. С увеличением длины последовательности $N$, смещение $B$ быстро уменьшается и значительно меньше соответствующего $3\sigma_B$-критерия, показанного на рис. 2, *б* пунктир-

ной линией. Для длины последовательности 10 Гбит значение $B \approx 10^{-6}$, что свидетельствует об отсутствии смещения. Это означает, что нет необходимости в использовании каких-либо дополнительных процедур постобработки на бинарном уровне. Полученная последовательность случайных бит характеризуется также отсутствием каких-либо существенных корреляций. На рисунке 3, *б* показаны первые 200 коэффициентов автокорреляции для последовательности длиной 10 Гбит. Практически все значения $C_k$ находятся в пределах диапазона, ограниченного пунктирными линиями, которые соответствуют $3\sigma_C$ -критерию.

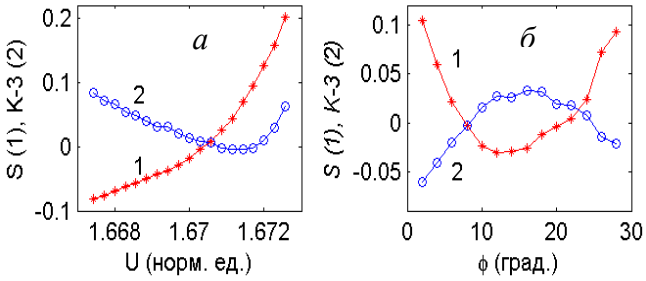


*Рис. 1*. Зависимость коэффициента асимметрии *S* и эксцесса *K* от нормированной амплитуды приложенного напряжения *U* (*а*); зависимость коэффициента асимметрии *S* и эксцесса *K* от угла поворота φ полуволновой пластины (*б*)

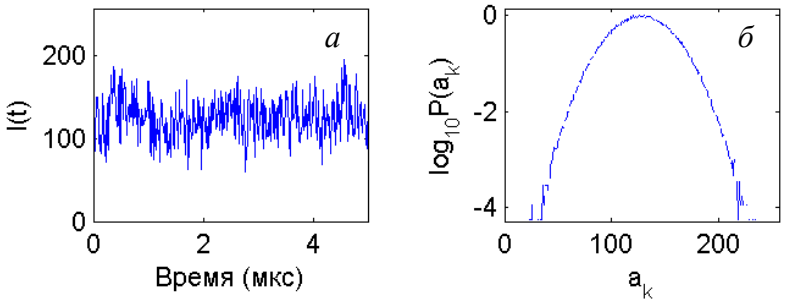


*Рис. 2.* Временное поведение лазерной интенсивности *I*(t) (*а*), функция плотности вероятности для измеренных амплитуд флуктуаций $a_k$ (*б*)

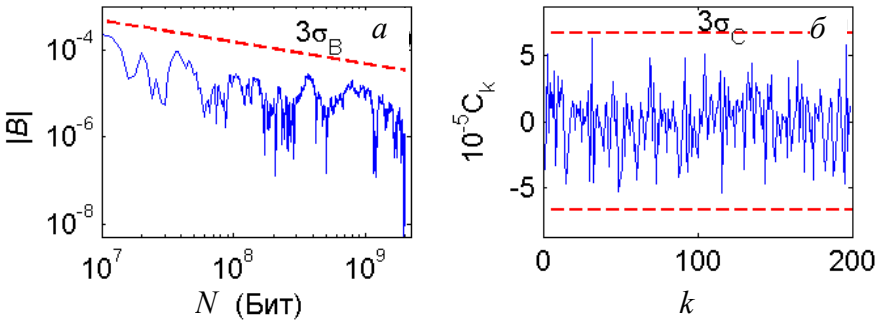


*Рис. 3.* Смещение *B* как функция числа сгенерированных бит *N* (*а*). Первые 200 коэффициентов автокорреляции для последовательности длиной 10 Гбит. Значения $C_k$ получены усреднением по ансамблю $10^4$ последовательностей 1 Мб каждая (*б*)

Дальнейшее статистическое испытание случайности последовательностей бит, сгенерированных этим методом, было выполнено с использованием трех наборов тестов, наиболее распространенных на практике для оценки качества случайных чисел: ENT-тест [12], набор тестов Национального бюро стандартов США (NIST) [13] и набор тестов Diehard [14]. С помощью указанных наборов тестов были протестированы 10 последовательностей длиной 1 Гбит каждая, которые были успешно пройдены. Таким образом, рассмотренный подход позволяет реализовать генерацию случайных бит со скоростью 100 Мбит/с.

Для увеличения скорости генерации бит был также применен недавно разработанный метод, основанный на вычислении финитной разности высокого порядка от исходных данных [11]. В отличие от работы [11], где функция распределения была существенно несимметричной, в данной работе этот метод применен к экспериментальным данным, для которых функция плотности вероятности распределения обладает достаточно высокой симметрией, в частности, коэффициент асимметрии $S \approx 0.001$. В работе использовался следующий алгоритм генерации бит. Вначале накапливалась последовательность 8-битных случайных целых чисел $\{a_k\}$ длины $N$. Затем, все целые случайные числа $a_k$ преобразовывались в числа с плавающей запятой (в этом случае максимальное число бит – 52). После этого находилась финитная разность $n$-го порядка $a_k^{(n)}$. Далее, все полученные числа преобразовывались в положительные числа и отображались в двоичный формат. Для построения бинарной последовательности извлекалось $l_b$ младших бит и добавлялись к ранее извлеченной $l_b$ –последовательности. При этом было найдено, что максимальное значение порядка финитной разности $n_{\max}$ и число извлеченных бит $l_b$ из каждого $a_k^{(n)}$, чтобы избежать появления корреляций в генерируемой последовательности случайных бит, должны удовлетворять условию: $n_{\max} \le 47$ и $l_b \le 46$. Детальное описание алгоритма приведено в [11]. Следует отметить, что применение финитной разности высокого порядка приводит к чрезвычайно высокой симметрии преобразованных данных (в частности, величина $S \approx 10^{-7}$) и увеличивает величину стандартного отклонения. Используя рассмотренный подход, из тех же данных была сгенерирована последовательность длиной 100 Гбит при $n = 47$ и извлечении 45 младших бит из каждого значения $a_k^{(n)}$. В этом случае эффективная скорость генерации составляет 4,5 Гбит/с. Для длины последовательности 100 Гбит было найдено, что величина статистического смещения $B<10^{-6}$ и максимальный коэффициент автокорреляции не превышает $C_k<10^{-5}$, что свидетельствует об отсутствии смещения и каких-либо существенных корреляций в произведенной последовательности бит. Аналогично, как и в первом случае, 10 последовательностей, длиной 1 Гб каждая, были успешно протестированы с использованием трех наборов тестов [12–14].

Таким образом, в работе экспериментально продемонстрировано, что поляризационный шум в лазере с вертикальным резонатором может быть использован в качестве источника энтропии для быстрой генерации высококачественных случайных бинарных последовательностей со скоростью генерации от 100 Мбит/с до 4,5 Гбит/с при применении постобработки, основанной на вычислении финитной разности высокого порядка. Последний метод может быть также полностью реализован на аппаратном уровне при использовании, например, программируемых логи-

ческих интегральных микросхем либо 64-битных процессоров цифровой обработки сигналов с плавающей запятой.

## ЛИТЕРАТУРА


1. *Knuth, D.* The art of computer programming (3rd edition)/ 1998. Vol. 2. Addison Wesley Longman.

2. *Walker, J.* Hotbits: Genuine random numbers, generated by radioactive decay / J. Walker // http://www.fourmilab.ch/hotbits.

3. *Stipcevic, M.* Fast nondeterministic random bit generator based on weakly correlated physical events / M. Stipcevic // Rev. Sci. Instrum. 2004. Vol. 75, №. 4. P. 4442–4445.

4. A fast and compact quantum random number generator / T. Jennewein [et al.] // Rev. Sci. Instrum. 2000. Vol. 71, №. 4. P. 1675 –1680.

5. *Stipcevic, M.* Quantum random number generator based on photonic emission in semiconductors / M. Stipcevic, B. M. Rogina //Rev. Sci. Instrum. 2007. Vol. 78, №. 4. P. 045104–7.

6. Fast physical random bit generation with chaotic semiconductor lasers / A. Uchida [et al.] // Nature Photonics. 2008. Vol. 2, № 12. P. 728–732.

7. *Reidler, I.* Ultrahigh-Speed Random Number Generation Based on a Chaotic Semiconductor Laser / I. Reidler, Y. Aviad, M. Rosenbluh, I. Kanter // Phys. Rev. Lett. 2009. Vol.103, № 2. 024102–4.

8. An optical ultrafast random bit generator / I. Kanter, Y. Aviad, I. Reidler [et al.] // Nature Photonics. 2010. Vol. 4. № 1. P. 58–61.

9. *Chizhevsky, V. N.* Random bits from quantum jumps / V. N. Chizhevsky, D. B. Horoshko, D. I. Pustakhod, S. Y. Kilin // Proceedings of SPIE. 2007. Vol. 6726. P. 67263N.

10. *Giacomelli, G.* Statistics of polarization competition in vcsels / G. Giacomelli, F. Marin // Quantum Semiclass. Opt. 1998. Vol. 10, № 3. P. 469–476.

11. *Chizhevsky, V. N.* Symmetrization of single-sided or non-symmetrical distributions: The way to enhance a generation rate of random bits from a physical source of randomness / V. N. Chizhevsky // Phys. Rev. E. 2010. Vol 82. № 5. P. 050101(R) –4.

12. *Walker, J.* Ent – a pseudorandom sequence test program, http://www.fourmilab.ch/random.

13. National Institut of Standards and Technology, Random number generation and testing, http://csrc.nist.gov/rng.

14. *Marsaglia, G.* The diehard test suite (2003), http://www.csis.hku.hk/~diehard/.