УДК 530.145

ВЛИЯНИЕ РАЗБРОСА ПАРАМЕТРОВ ЭКСПЕРИМЕНТА НА СТАТИСТИЧЕСКИЕ ХАРАКТЕРИСТИКИ КВАНТОВОГО ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ

© 2014 г. **А. Е. Иванова**, аспирант; **С. А. Чивилихин**, канд. физ.-мат. наук; **Г. П. Мирошниченко**, доктор физ.-мат. наук; **В. И. Егоров**, аспирант; **А. В. Глейм**, аспирант

Университет ИТМО, Санкт-Петербург

E-mail: newiva@mail.ru

Квантовая генерация случайных чисел позволяет получить истинно случайные числа, которые могут использоваться в приложениях, где необходима высокая степень случайности. В данной работе проводится оценка влияния неидеальности параметров схем на результаты проводимых измерений для двух схем квантовой генерации случайных чисел: основанной на разделении лазерного излучения и основанной на использовании вакуумных флуктуаций.

Ключевые слова: *генерация случайных чисел, светоделитель, гомодинное детектирование.*

Коды OCIS: 270.0270, 270.5290, 270.5565.

Поступила в редакцию 09.04.2014.

Введение

Генерация случайных чисел может осуществляться алгоритмически, однако получаемые последовательности псевдослучайны по своей природе и не подходят для приложений, в которых необходима высокая степень случайности, таких как квантовая криптография [1]. Для этих приложений необходимо использовать истинно случайные числа, получаемые с помощью недетерминированных физических процессов [2], в том числе квантовых [3].

Существующие подходы к реализации квантовой генерации случайных чисел включают использование запутанных фотонных состояний [4], процессов фотонного излучения и обнаружения [5], квантового шума лазера [6], разделения излучения [7]. Альтернативным подходом является использование вакуумных флуктуаций электромагнитного поля [8, 9].

Практическая реализация любого генератора случайных чисел отличается по характеристикам от его теоретического описания. Следовательно, важно промоделировать влияние любых возможных сбоев и изучить их воздействие на статистические характеристики получаемых результатов. В данной работе исследуется случай отклонения угла θ светоделителя от значения $\theta = 45°$ и квантовой эффективности детекторов. Расчеты выполнены для двух различных методов генерации: первый основан на разделении лазерного излучения, второй – на использовании статистики флуктуаций вакуума при гомодинном детектировании.

Квантовая генерация случайных чисел, основанная на разделении излучения с помощью светоделителя

При исследовании статистики распределения, полученного с использованием светоделителя, была проведена симуляция вероятностного процесса. В данной схеме генерации случайных чисел (рис. 1) лазерное излучение

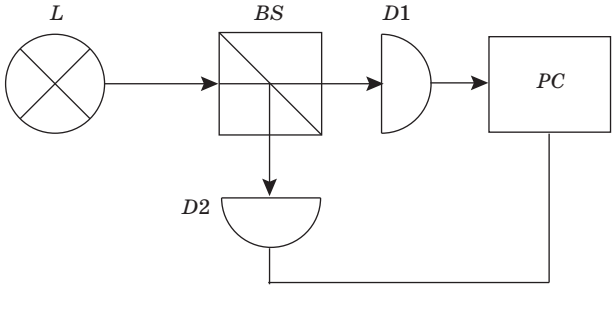

Рис. 1. Схема генерации случайных чисел, основанная на разделении излучения с помощью светоделителя. *L* – лазер, *BS* – светоделитель, *D*1, *D*2 – детекторы, *PC* – компьютер.

разделяется с помощью светоделителя и регистрируется детекторами. Показано, что если лазерное излучение, определяемое пуассоновским распределением с параметром α (описывающим среднее число фотонов), проходит через светоделитель с углом θ, то на одном из выходов светоделителя пуассоновское распределение будет иметь параметр $\alpha_1 = \alpha\cos\theta$, а на другом – параметр $\alpha_2 = \alpha\sin\theta$.

Обработка двух последовательностей, полученных после разделения исходного излучения, происходит следующим образом: если на первом выходе из светоделителя не были обнаружены фотоны, а на втором обнаружено любое их количество, то бит итоговой последовательности принимает значение «0», в противоположном случае, т.е. если на первом выходе были обнаружены фотоны, а на втором – нет, – «1» , в остальных случаях бит не записывается.

Было показано, что для несимметричного светоделителя степень равномерности итогового распределения зависит от угла светоделителя. С увеличением отклонения угла светоделителя (от значения $\theta = 45°$) мы увеличиваем разницу вероятностей генерации единиц и нулей в итоговой последовательности. Необходимо рассчитать отклонение угла светоделителя, при котором итоговая битовая последовательность является случайной. Статистические параметры бинарного распределения, полученного для асимметричного светоделителя, показаны на рис. 2. Сгенерированные последовательности успешно проходят тесты на случайность, если отклонение от угла $\theta = 45°$ составляет не более двух градусов.

Параметры детекторов влияют на качество сгенерированных последовательностей случайных чисел. В случае, когда квантовые эффективности детекторов равны, некоторые случайные отсчеты в обеих последовательностях, полученных на выходе светоделителя, обнуляются и тогда качество итоговой последовательности не падает, поскольку изменения случайны и квантовые эффективности детекторов одинаковы. Мы также рассматривали ситуацию, когда квантовые эффективности двух детекторов различны. В этом случае одна из последовательностей на выходе светоделителя будет содержать большее количество нулевых отсчетов, чем другая. Различие параметров детекторов изменяет соотношение нулей и единиц в итоговой последовательности, оказывая влияние на ожидаемое для данного угла светоделителя качество получаемой в итоге последовательности. Рисунок 3 показывает вероятности получения битов «0» или «1» в зависимости от соотношения вероятностей детектирования первого и второго детекторов (P_1 и P_2).

Из приведенных зависимостей видно, что асимметрия детекторов может скомпенсировать различие в вероятностях из-за асимметрии светоделителя при правильном подборе параметров. Например, если после разделения пучка в одной из последовательностей число ненулевых отсчетов больше, чем в другой, но она детектируется с помощью устройства с бóльшим числом нулевых отсчетов, то в итоговой последовательности битов может быть достигнут требуемый баланс между вероятностями появления нулей и единиц.

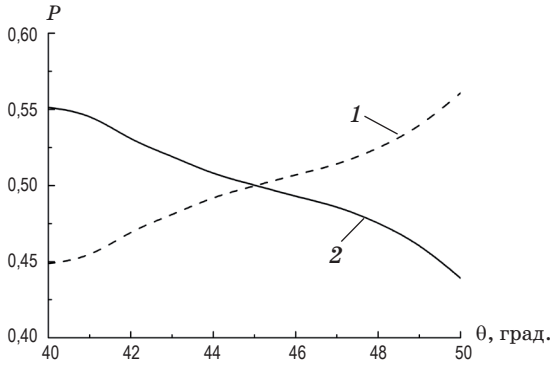

Рис. 2. Параметры бинарного распределения для асимметричного светоделителя. Вероятности (*P*) появления нулей (*1*) и единиц (*2*) в итоговой последовательности в зависимости от угла светоделителя θ.

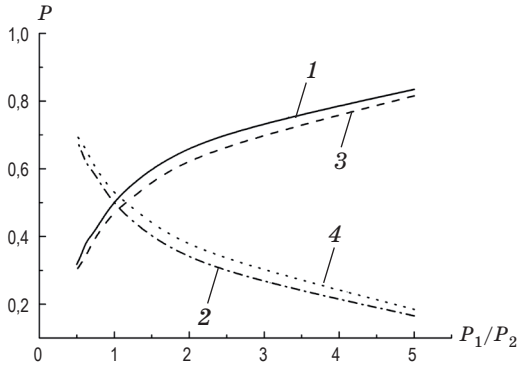

Рис. 3. Зависимости вероятности *P* появления битов “0” (*1*) и “1” (*2*) при использовании симметричного светоделителя от соотношения параметров детекторов; зависимости вероятности появления битов “0” (*3*) и “1” (*4*) при использовании светоделителя с углом $\theta = 50°$ от соотношения параметров детекторов. Вероятность детектирования на первом детекторе $P_1 = 10\%$.

Квантовая генерация случайных чисел, основанная на принципах гомодинного детектирования

Принципом работы данной схемы является извлечение последовательности случайных чисел из квантового шума, который появляется при вычитании сигналов, поступающих с выходов светоделителя (рис. 4).

На один из входов светоделителя подается световой импульс в когерентном состоянии, а на другой – электромагнитный вакуум. В этом случае в светоделителе происходит взаимодействие между сильным лазерным сигналом и флуктуациями вакуума. Случайные числа являются результатом обработки полученного разностного сигнала. Сигналы (операторы) на входах и выходах светоделителя обозначены a_1, a_2 и b_1, b_2 соответственно (рис. 5).

Операторы на входах и выходах связаны между собой следующим образом:

$$\begin{cases} b_1 = a_1 \cos\theta - a_2 \sin\theta, \\ b_2 = a_1 \sin\theta + a_2 \cos\theta. \end{cases}$$

Импульс лазерного излучения характеризуется пуассоновским процессом с параметром α и определяется как

$$|\alpha\rangle = \exp\left(\alpha a_1^+ - \alpha^* a_1\right)|0\rangle,$$

где a_1^+ и a_1 – операторы рождения и уничтожения фотонов на первом входе светоделителя, $|\alpha\rangle$ – когерентное состояние, $|0\rangle$ – вакуумное состояние.

Если на один вход светоделителя подается сигнал состояния вакуума $|0\rangle$, а на другой – когерентного состояния $|\alpha\rangle$, то входной сигнал выражается в виде тензорного произведения

$$|\alpha\rangle\,|0\rangle = \exp\left(\alpha a_1^+ - \alpha^* a_1\right)|0\rangle_1 |0\rangle_2.$$

После прохождения излучения, определяемого пуассоновским распределением с параметром $|\alpha\rangle$, через светоделитель с углом θ на одном из выходов светоделителя пуассоновское распределение определяется параметром $|\alpha\cos\theta\rangle$, а на другом – параметром $|\alpha\sin\theta\rangle$.

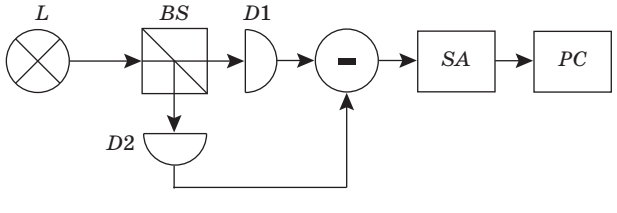

Рис. 4. Схема генерации случайных чисел, основанная на принципе гомодинного детектирования. *SA* – спектроанализатор. Обозначения остальных элементов – см. подпись к рис. 1.

Предположим, что фотодетекторы работают в квантовом режиме, проводя счет падающих на (условно) первый и (условно) второй фотодетектор фотонов. Скорости счета фотонов определяются соотношениями

$$V_1 = \gamma_1 \left\langle b_1^+ b_1 \right\rangle,\ V_2 = \gamma_2 \left\langle b_2^+ b_2 \right\rangle,$$

где γ_1 и γ_2 – квантовые эффективности первого и второго детекторов соответственно, скобки означают усреднение по начальному состоянию излучения. Сопоставим фотону первого фотодетектора бит, равный 0, а второму – равный 1. Вероятности “0” и “1” битов определим соотношениями

$$P_1 = \frac{V_1}{V_1 + V_2},\ P_2 = \frac{V_2}{V_1 + V_2}.$$

Скорости счета фотонов равны

$$V_1 = \alpha^2 \gamma_1 \cos^2\theta,\ \ V_2 = \alpha^2 \gamma_2 \sin^2\theta.$$

Отсюда вероятности битов –

$$P_1 = \frac{\gamma_1 \cos^2\theta}{\gamma_1 \cos^2\theta + \gamma_1 \sin^2\theta},\ P_2 = \frac{\gamma_2 \sin^2\theta}{\gamma_1 \cos^2\theta + \gamma_1 \sin^2\theta}.$$

Очевидно, выборка случайной последовательности битов всегда конечна. Обозначим длину выборки N и оценим качество выборки с помощью следующего критерия. Найдем максимально вероятное число битов “0”, проанализировав серию выборок объема N, и обозначим его $N_{\max}^0$. Определим отклонение ΔP вероятностей P_0, P_1 от 0,5.

$$P_1 = \frac{1}{2} + \Delta P,\ P_2 = \frac{1}{2} - \Delta P.$$

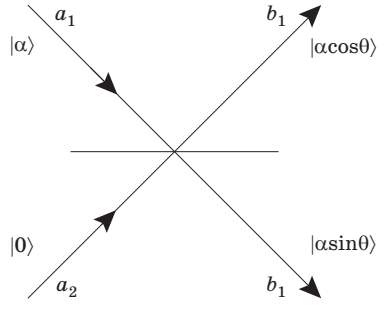

Рис. 5. Схема светоделителя с углом θ, где на первый вход подается световой импульс в когерентном состоянии, а на другой – электромагнитный вакуум (пояснения в тексте).

Используя биномиальное распределение, получим

$$(N+1)\Delta P-\frac{1}{2}\le N^0_{\max}-\frac{N}{2}\le(N+1)\Delta P+\frac{1}{2}.$$

Выборку можно считать идеальной, если

$$\left|N^0_{\max}-\frac{N}{2}\right|\le\frac{1}{2}.$$

Тогда качество выборки объема N для неидеальной экспериментальной установки можно оценить по формуле

$$\Delta P\le\frac{1}{2(N+1)}.$$

Обозначим отклонения эффективностей детекторов как

$$\gamma_1=\gamma+\Delta\gamma_1,\quad \gamma_2=\gamma+\Delta\gamma_2,$$

а отклонение угла светоделителя –

$$\theta=\pi/4+\Delta\theta.$$

Тогда отклонение вероятностей P_0, P_1 от 0,5 определяется формулой

$$\Delta P_2=-\Delta P_1=\frac{|\Delta\gamma_1|+|\Delta\gamma_2|}{\gamma}+|\Delta\theta|.$$

Качество выборки объема N по исследуемому критерию будет обеспечено, если выполнено условие

$$\frac{|\Delta\gamma_1|+|\Delta\gamma_2|}{\gamma}+|\Delta\theta|\le\frac{1}{2(N+1)}.$$

Заключение

Проведено исследование влияния неидеальности элементов схем квантовой генерации случайных чисел на результаты измерений. Рассмотрены два типа генерации, основанные на разделении лазерного излучения и на флуктуациях вакуума. Показано, что последовательности, сгенерированные с помощью разделения пучка, успешно проходят тесты на случайность, если отклонение угла делителя пучка составляет не более двух градусов. Определено, что в общем случае асимметрия параметров детекторов ухудшает качество генерируемых последовательностей, но при корректном подборе параметров может скомпенсировать асимметрию делителя пучка. Для схемы квантовой генерации случайных чисел с помощью гомодинного детектирования получены выражения, описывающие взаимосвязь между излучением, падающим на светоделитель, и излучением, регистрируемым разностным током. Найдены соотношения, позволяющие оценить влияние неидеальности элементов схемы на результаты измерений.

Работа выполнена при государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01, проект 14.Z50.31.0031).

* * * * *

ЛИТЕРАТУРА

1. *Scarani V., Bechmann–Pasquinucci H., Cerf N. J., Dušek M., Lütkenahus N. and Peev M.* The security of practical quantum key distribution // Rev. Mod. Phys. 2009. V. 81. P. 1301–1350.
2. *Argyris A., Deligiannidis S., Pikasis E., Bogris A., and Syvridis D.* Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit // Optics Express. 2010. V. 18. № 18. P. 18763–18768.
3. *Jennewein T., Achleitner U., Weihs G., Weinfurter H., and Zeilinger A.* A fast and compact quantum random number generator // Rev. Sci. Instrum. 2000. V. 71. № 4. P. 1675–1680.
4. *Kwon O., Cho Y.-W. and Kim Y.-H.* Quantum Random Number Generator using Photon-Number Path Entanglement // Appl. Opt. 2009. V. 48. P. 1774–1778.
5. *Stipčević M. and Rogina M. B.* Quantum random number generator based on photonic emission in semiconductors // Rev. Sci. Instrum. 2007. V. 78. P. 045104.
6. *Qi B., Chi Y.-M., Lo H.-K. and Qian L.* High-speed quantum random number generation by measuring phase noise of a single-mode laser //Optics Letters. 2010. V. 35. № 3. P. 312–314.
7. *Ivanova A. E., Egorov V. I., Chivilikhin S. A. and Gleim A. V.* Investigation of quantum random number generation based on space-time division of photons // Nanosist.:phys. chem. mat. 2013. V. 4. № 4. P. 550–554.
8. *Shen Y., Tian L., Zou H.* Practical quantum random number generator based on measuring the shot noise of vacuum states // Phys. Rev. 2010. V. 81. P. 063814.1-5.
9. *Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Mauerer, Ulrik L. Andersen, Christoph Marquardt and Gerd Leuchs.* A generator for unique quantum random numbers based on vacuum states // Nature Phot. 2010. V. 4. P. 711–715.