Обзор аппаратных генераторов случайных чисел

Подорожный Иван Вадимович, магистр
Московский государственный технический университет имени Н.Э. Баумана

Данная статья посвящена исследованию основных способов построения аппаратных генераторов случайных чисел. Рассмотрены их схемы и отличительные способности. В заключении статьи приведен краткий вывод.

Ключевые слова: *генератор случайных чисел, квантовый генератор, тепловой шум.*

Генераторы, использующие физические квантовые случайные процессы

Фазовый квантовый шум в лазерном луче

Одним из самых надежных способов получения случайных чисел является ГСЧ, регистрирующий квантовый эффект удара фотонов в зеркало.

На полупрозрачное зеркало направляются фотоны, генерируемые источником одиночных фотонов. Фотон может отразиться, а может пройти через полупрозрачное зеркало с одинаковыми долями вероятности. Выбор, который «делает» фотон, абсолютно случаен. На выходе системы стоят два счетчика фотонов, регистрирующих прошедшие и отраженные фотоны и формирующих выходные электрические сигналы. [1]

Подобные квантовые генераторы имеют высокую скорость выходного потока — до 10–16 Мбит/с, — при которой не наблюдается никаких корреляций и выполняются все статистические тесты. [2]

Матрица фотокамеры

Большинство источников света выпускают фотоны в совершенно случайные моменты времени и количество фотонов, выпущенных за единицу времени будет различаться на величину, которая является полностью случайной. Этот факт лег в основу ГСЧ, построенного на базе светочувствительной КМОП-матрицы обычной фотокамеры группой ученых из Женевского университета во главе с Бруно Сангинетти.

Каждый пиксель матрицы «считает» количество фотонов, попавших на его поверхность за определенный промежуток времени. Эти фотоны конвертируются в электроны, которые затем умножаются на множитель, определенный светочувствительностью матрицы (уровень ISO). Количество электронов за один и тот же период будет отличаться на совершенно случайное число.

На практике процесс генерации таких случайных чисел выглядит довольно просто: матрица фотокамеры засвечивается зеленым светодиодом и делаются два снимка с одинаковой длительностью выдержки. Затем снимки программно обрабатываются для получения случайных чисел.

По словам разработчиков, случайные числа, полученные в результаты опытов с использованием светочувствительной матрицы современного мобильного телефона, успешно прошли статистические тесты. Более того, за счет больших размеров матрицы и частоты получения снимков, разработанный ими ГСЧ может генерировать случайные числа с огромной скоростью (до 3 Гбит/с). [3]

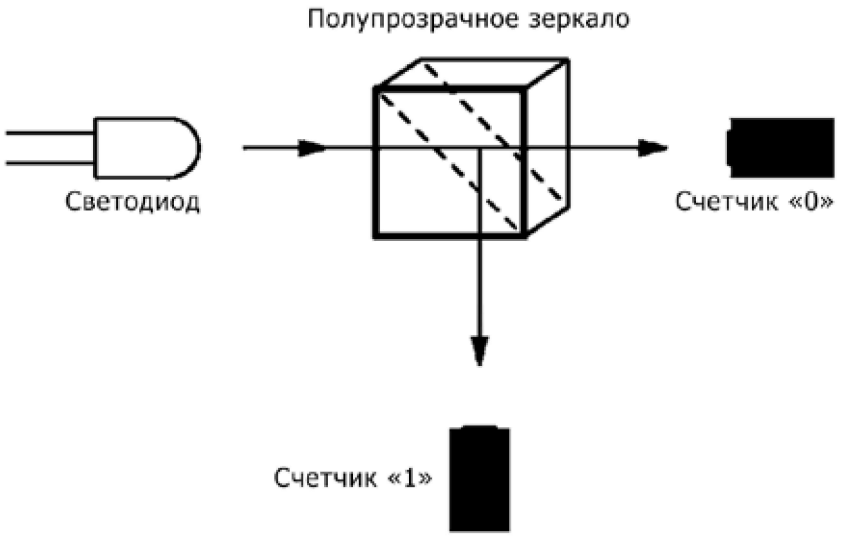

Рис. 1. **Схема ГСЧ, построенного на базе фазового квантового шума в лазерном луче**

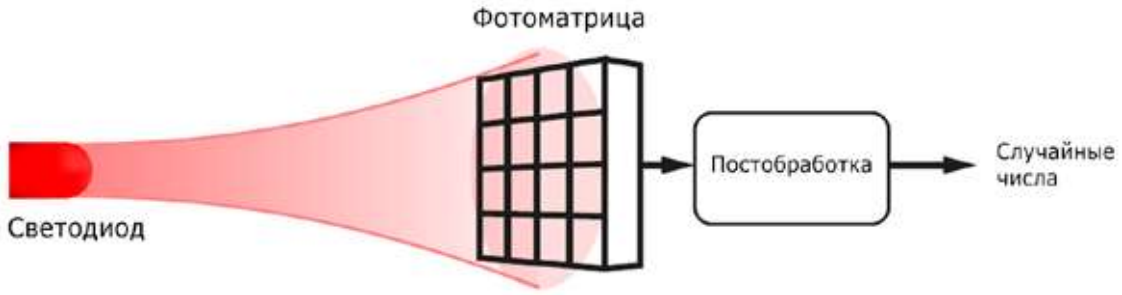

Рис. 2. **Схема ГСЧ, построенного на базе фотоматрицы**

Генераторы, использующие другие физические случайные процессы

Тепловой шум

Тепловой шум, также называемый шумом Джонсона, генерируется всеми пассивными резистивными элементами электрических цепей. Причина его появления — случайное броуновское движение электронов в резистивной среде. Тепловой шум увеличивается с ростом температуры и сопротивления и часто оказывается самой существенной составляющей шума в прецизионных полупроводниковых преобразователях данных. [4]

Одним из успешных примеров построения ГСЧ на базе теплового шума является генератор, разработанный компанией Intel в 1999 году и используемый в чипсетах Intel 800 серии.

ГСЧ Intel использует последовательности случайных чисел, получаемые с двух тактовых генераторов, частота работы одного из которых превышает частоту другого в 100 раз. Тепловой шум с источника (полупроводникового резистора) усиливается и используется для управления частотой колебаний медленного генератора.

Случайные числа, полученные в результате дрейфа (погрешности хода) двух генераторов, проходят дальнейшую аппаратную обработку через «корректор Фон Неймана» для получения сбалансированного распределения нулей и единиц.

Среди недостатков данного генератора случайных чисел можно выделить большое энергопотребление (из-за кольцевого генератора, используемого для усиления теплового шума) и относительно небольшую для современных потребностей скорость генерации (порядка 75 Кбит/с после пост-обработки). [5]

Цифровая схема с неопределенным состоянием

В 2008 году инженеры компании Intel принялись за разработку нового варианта генератора случайных чисел, который работает исключительно на цифровой основе.

Предложенное ими решение нарушает основное правило цифрового проектирования: схема всегда должна

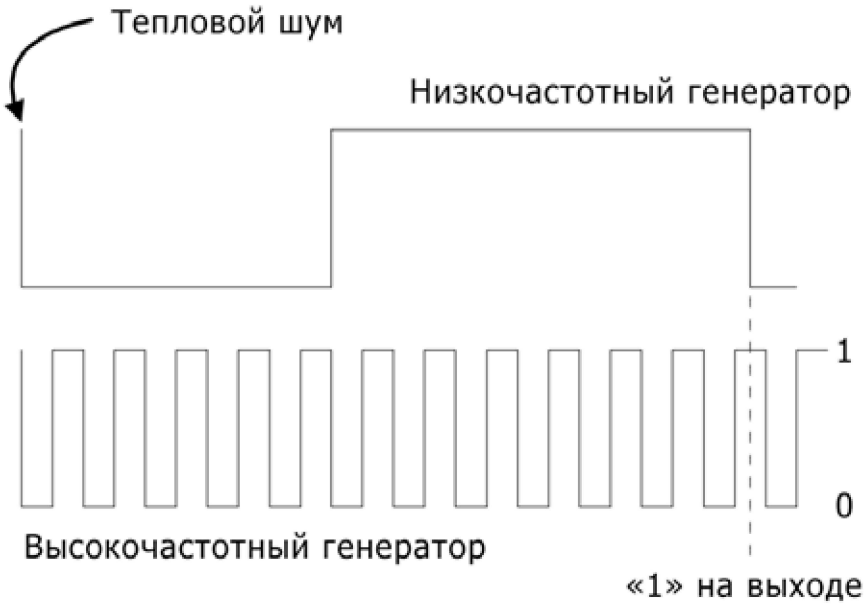

Рис. 3. **Временная диаграмма ГСЧ Intel**

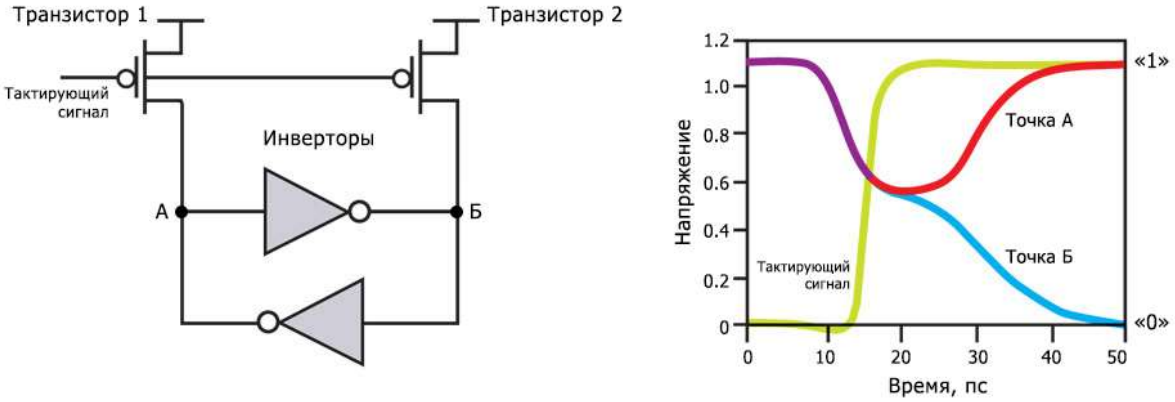

Рис. 4. **Современный генератор Intel**

быть в одном из двух определенных состояний (логический низкий и логический высокий уровни сигнала).

Схема ГСЧ состоит из пары инверторов, выход каждого из которых подключен к входу другого. Если на выходе у первого инвертора будет логический низкий уровень сигнала, то второй инвертор получит этот уровень на входе и, соответственно, выдаст высокий уровень сигнала на выходе, и наоборот. Дополнительно в цепь добавлены два транзистора, включение которых дает на входе и выходе обоих инверторов логический высокий сигнал. Каждый период тактирующего сигнала, при отключении транзисторов, оба инвертора стремятся принять противоположное положение, т. е. одно из двух устойчивых состояний, генерируя при этом один случайный бит.

Данная разработка позволила избавиться от неудобств аналоговых компонентов предыдущего варианта ГСЧ, значительно уменьшить энергопотребление и увеличить скорость генерации более чем в 30 тысяч раз. [6]

Лавинный шум (шум лавинного умножения)

Источниками лавинного шума являются PN-переходы, работающие в режиме обратного пробоя, как это происходит в стабилитронах (зенеровских диодах). Ток, генерируемый во время лавинного пробоя, состоит из случайно распределённых шумовых выбросов, проходящих через обратно смещённый переход. Подобно дробовому шуму, для генерации лавинного шума требуется наличие тока, но обычно он гораздо интенсивнее. [4]

В ГСЧ на базе такого источника случайных чисел обычно используют переход эмиттер-база биполярного NPN транзистора из-за низкого пробойного напряжения. Снятый с перехода шум усиливается и преобразовывается в цифровой сигнал.

Случайные числа с подобных ГСЧ проходят все статистические тесты, однако скорость их генерации крайне мала — менее 10 Кбит/с. [7]

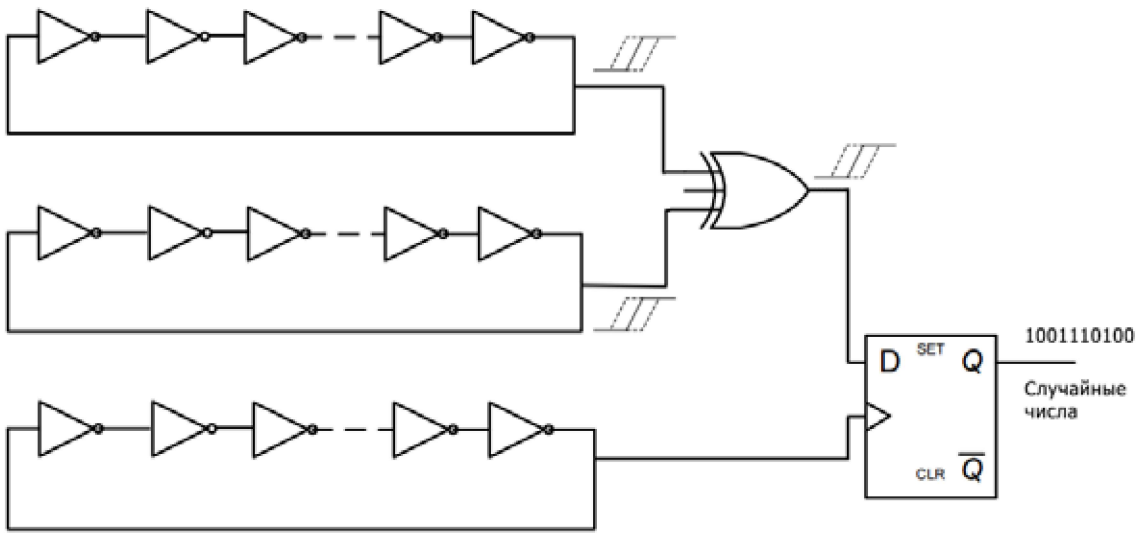

Рис. 5. **ГСЧ, построенный на кольцевых генераторах**

Фазовое дрожание в кольцевых генераторах

Фазовое дрожание цифрового сигнала данных (джиттер от англ. jitter) — нежелательные фазовые и/или частотные случайные отклонения передаваемого сигнала. Возникают вследствие нестабильности задающего генератора, изменений параметров линии передачи во времени и различной скорости распространения частотных составляющих одного и того же сигнала. Поскольку фазовое дрожание зависит от различных факторов, некоторые из которых полностью случайны, оно может быть использовано как источник случайных чисел. [8]

В ГСЧ на базе такого явления обычно сравниваются случайные задержки прохождения сигнала через кольцевые генераторы. Простейший кольцевой генератор состоит из нечетного числа инверторов, соединенных последовательно, при этом выход последнего соединен с входом первого инвертора, образуя линию обратной связи. Частота колебания такого генератора определяется суммой задержек всех его инверторов, это время зависит от множества параметров, включающих в себя тепловой шум в проводниках и полупроводниках и помехи в источниках питания. [9]

Среди минусов такого ГСЧ можно выделить относительно небольшую скорость генерации и большое энергопотребление.

Заключение

В статье были рассмотрены основные способы построения аппаратных генераторов случайных чисел. Среди них можно выделить один из самых современных и прогрессивных способов — генератор случайных чисел на базе неопределенных состояний, разработанный инженерами компании Intel и обладающий одной из самых высоких скоростей выходного потока (до 3 Гбит/с) и низким энергопотреблением.

Литература:

1. Задков Виктор, Владимирова Юлия. Классические и квантовые генераторы случайных чисел. URI: http://www.supercomputers.ru/index. php?id=441&option=com_k2&view=item (дата обращения: 17.12.2015).
2. M. Stipčevića, B. Medved Rogina. Quantum random number generator based on photonic emission in semiconductors. URI: http://www-personal.umich.edu/~andrewcb/DSO/Papers/Random Number Generator/2007-quantum_random_number_generator_based_on_photonic_emission. pdf (дата обращения: 17.12.2015).
3. Anthony Martin, Hugo Zbinden, Nicolas Gisin. Quantum random number generation on a mobile phone. URI: http://arxiv.org/pdf/1405.0435v1. pdf (дата обращения: 17.12.2015).
4. Стив Эдвардс. Оптимизация шумовых параметров сигнальных цепей. URI: http://www.symmetron.ru/articles/noise-reduction-1. pdf (дата обращения: 17.12.2015).
5. Benjamin Jun, Paul Kocher. The Intel random number generator. URI: https://www.rambus.com/wp-content/uploads/2015/08/IntelRNG. pdf (дата обращения: 17.12.2015).
6. Greg Taylor, George Cox. Behind Intel's new random number generator. URI: http://spectrum.ieee.org/computing/hardware/behind-intels-new-randomnumber-generator (дата обращения: 17.12.2015).
7. Holden. Random sequence generator based on avalanche noise. URI: http://holdenc.altervista.org/avalanche/(дата обращения: 17.12.2015).
8. Vikram Belur Suresh. On-chip true random number generation in nanometer CMOS. URI: http://scholarworks.umass.edu/cgi/viewcontent. cgi?article=1872&context=theses (дата обращения: 17.12.2015).
9. Прощеряков, А.А., Иванюк А.А. Кольцевой генератор и его неповторимый температурный коэффициент линейной регрессии. URI: http://libeldoc.bsuir.by/bitstream/123456789/3312/1/Кольцевой генератор и его неповторимый температурный коэффициент линейной регрессии. PDF (дата обращения: 17.12.2015).