ОБЗОР ПРИНЦИПОВ РАБОТЫ И ФАКТОРОВ, ВЛИЯЮЩИХ НА КАЧЕСТВО ФИЗИЧЕСКИХ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ЧИСЕЛ

Диско А.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Михневич С.Ю. – канд. физ.-мат. наук, доцент кафедры ИРТ

Рассмотрены принципы построения физических и квантовых генераторов случайных чисел, их характеристики и влияние внешних факторов на качество генерации.

Введение: Случайные числа являются критически важным ресурсом для систем криптографической защиты информации, моделирования сложных процессов и научных экспериментов. В отличие от программных генераторов псевдослучайных чисел, физические генераторы используют фундаментально непредсказуемые процессы, что делает их незаменимыми в приложениях, требующих высокой степени энтропии. Настоящая работа посвящена зависимостям генераторов случайных чисел от внешних условий.

Принципы построения генераторов случайных чисел: Одним из первых исторических подходов является использование радиоактивного распада. Время между последовательными распадами подчиняется экспоненциальному распределению и статистически независимо, что позволяет формировать случайные биты путём сравнения временных интервалов или подсчёта числа импульсов за фиксированный период. Однако низкая скорость генерации (до сотен килобит в секунду) и необходимость использования радиоактивных материалов ограничивают практическое применение этого метода [1].

Шумовые генераторы, построенные на основе полупроводниковых элементов (стабилитронов, транзисторов, шумовых диодов), используют дробовой или тепловой шум. Дробовой шум имеет квантовое происхождение и связан с дискретностью носителей заряда, тогда как тепловой шум обусловлен хаотическим движением носителей и зависит от температуры. В реальных устройствах эти два типа шума присутствуют совместно, что затрудняет изоляцию чисто квантовой составляющей. В некоторых коммерческих реализациях, например в генераторе компании ComScire, выполняется детальная оценка квантовой энтропии, получаемой из дробового шума в МОП-транзисторах [1].

Наиболее перспективными и быстроразвивающимися являются оптические квантовые генераторы случайных чисел. Они используют различные квантовые эффекты: случайность пути фотона на светоделителе, флуктуации времени прихода фотонов, квантовые вакуумные флуктуации, фазовый шум лазеров, усиленное спонтанное излучение, а также эффекты комбинационного рассеяния [1]. Скорости генерации в таких устройствах достигают десятков гигабит в секунду, что делает их пригодными для высокоскоростных криптографических приложений.

Влияние внешних условий на характеристики генераторов: температура окружающей среды изменяет физические параметры полупроводниковых компонентов. В полупроводниковых шумовых диодах с ростом температуры увеличивается напряжение пробоя, уменьшается длина свободного пробега носителей заряда, что приводит к изменению шумовых характеристик. В случае оптических систем температурный дрейф влияет на характеристики как источников излучения (лазеров, светодиодов), так и фотоприёмников, что может приводить к изменению эффективности регистрации и появлению систематических смещений [1].

Электрический режим работы является критическим параметром для полупроводниковых генераторов. Для шумовых диодов существует оптимальный диапазон обратного тока, в котором спектральная плотность шума наиболее равномерна. Выход за пределы этого диапазона приводит к возрастанию неравномерности спектра и появлению корреляций, что снижает энтропию выходной последовательности [1].

Освещённость и стабильность источника света в оптических системах вносят классическую составляющую в измеряемый сигнал. Любая измерительная система может вносить смещение (bias), если на результат измерений влияют неквантовые факторы [2]. Изменение уровня освещённости, нестабильность светодиода или температурный дрейф характеристик матрицы камеры могут приводить к тому, что распределение регистрируемых значений отклоняется от теоретически ожидаемого. Если фиксировать по среднему значению, получаем кривую, которая несбалансированна по количеству “0” и “1”. На рисунке 1 представлена зависимость результата битового теста (т.е. сумма случайность последовательности, в которой «0» принимается за «-1»), а ось Ox представляет собой функцию зависящую от внешних условий (температура, давление, освещенность),. Видно что при изменении внешних условия у нас могут превалировать или “0” или “1”.

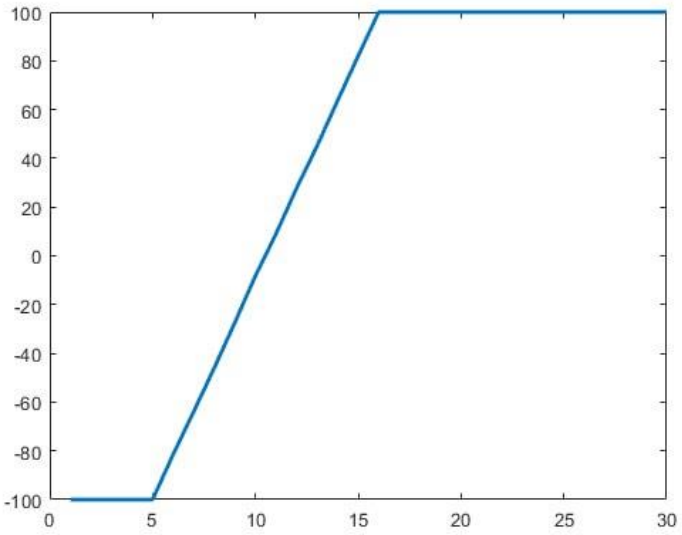

Рисунок 1 – битовый тест на случайность от внешних условий.

Как видно на рисунке 1, значение битовых “1” превышает значение битовых “0”, для восстановления баланса битовых “0” и “1” вводится дополнительный узел, увеличивающий время генерации, уязвимость к криптоатакам и вносящий дополнительный источник ошибки. Для этого предлагается работать в области оптической бистабильности, где количество битовых “0” и “1” не зависит от внешних условий.

Заключение: физические генераторы случайных чисел, являются критически важными для криптографии и фундаментальных научных экспериментов. Наиболее перспективными признаны оптические квантовые генераторы, достигающие скоростей до десятков гигабит в секунду и допускающие интеграцию на одном чипе стоимостью несколько долларов, что открывает путь к массовому внедрению истинно случайных чисел в мобильные устройства и системы интернета вещей. Внешние факторы, такие как температура, электрический режим и стабильность источника света, способны влиять на качество генерации, что требует применения методов постобработки для обеспечения криптографической стойкости выходных последовательностей или реализация режимов генерации невосприимчивых к изменению внешних условий в каком-то диапазоне.

Список использованных источников:

[1] Herrero-Collantes, M. Quantum random number generators / M. Herrero-Collantes, J. C. Garcia-Escartin // Reviews of Modern Physics. – 2016. – Vol. 89. – pp. 2-28.

[2] Johnston, H. How to make a quantum random-number generator from a mobile phone / H. Johnston // Physics World. – 2014. – Режим доступа: https://physicsworld.com/a/how-to-make-a-quantum-random-number-generator-from-a-mobile-phone/. – Дата доступа: 24.03.2026.