Литература

1. Nirav Mehta. Choosing an Open Source CMS. Beginner's Guide. — Packt (англ.)русск., April 2009. — 340 p. — ISBN 978-1-847196-22-4.

УДК 621.382

ФИЗИЧЕСКИЙ ГЕНЕРАТОР СЛУЧАЙНЫХ ЧИСЕЛ ДЛЯ ФОРМИРОВАНИЯ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ НА БАЗЕ ФОТОМАТРИЦЫ

студент гр. 10306115 Бурый А. В.
Научный руководитель - к.т.н., доцент Гулай А. В.
Белорусский национальный технический университет
Минск, Беларусь

Ранее криптография служила только интересам государства, но с появлением интернета ее методы стали интересовать и частных лиц. На сегодняшний день криптография широко используется в различных сферах, однако в большинстве случаев цель использования, это защита информации.

В основе криптографии лежат криптографические ключи, представляющие секретную информацию, используемую криптографическим алгоритмом при шифровании и расшифровывании различных данных. В крупных информационных сетях возникает необходимость генерации большого количества криптографических ключей, которые не должны повторяться. Для выполнение данной задачи используются различные генераторы случайных чисел. [1]

Существует большое количество различных физических генераторов случайных чисел, в основе которых лежать различные хаотически изменяющиеся параметры протекающего физического процесса. В рамках данной статьи рассмотрен физический генератор случайных чисел для формирования криптографических ключей на базе фотоматрицы, который представлен на рисунке ниже.

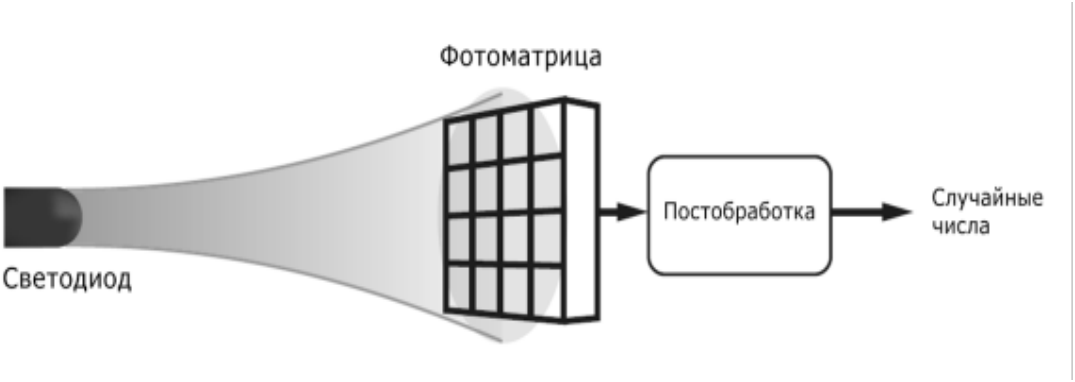

Рис. 1. Схема генератора случайных чисел, построенного на базе фотоматрицы

Основными рабочими элементами представленного выше генератора является светодиод и фотоматрица. Принцип работы такого генератора случайных чисел основан на подсчете эмиссии фотона. Этот квантовый процесс по своей природе случаен, поскольку в конкретный промежуток времени от источника света получается случайное количество фотонов. [2]

Каждый пиксель матрицы определяет 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 светодиодом и делаются два снимка с одинаковой длительностью выдержки. Затем снимки программно обрабатываются для получения случайных чисел. [3]

Данный генератор является полностью совместимым в интегральные микросхемы, имеет малые габариты и высокую надежность. Генератор позволяет получать последовательности случайных чисел со скоростью от 1 до 75 мегабит, в зависимости от характеристик используемых компонентов.

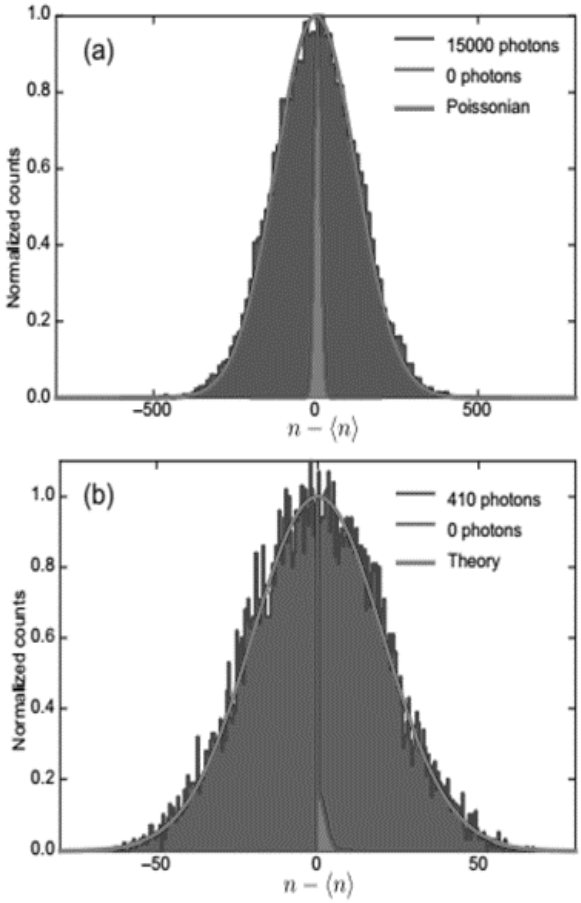

Рис. 2. Распределение случайных величин генератора на основе 8 Мп камеры с оптикой Carl Zeiss

Распределение полученных случайных величин соответствует распределению Гаусса. Генератор на основе 8 Мп камеры с оптикой Carl Zeiss даёт лишь одно отклонение от идеальной случайной последовательности на 1096 итераций, представлено на рисунке 2. [3]

Литература

1. Дошина А. Д., Михайлова А. Е., Карлова В. В. Криптография. Основные методы и проблемы. Современные тенденции криптографии [Текст] // Современные тенденции технических наук: материалы IV Междунар. науч. конф. (г. Казань, октябрь 2015 г.). — Казань: Бук, 2015.

2. Подорожный И. В. Обзор аппаратных генераторов случайных чисел // Молодой ученый. — 2016.

3. «Хабр» — крупнейший в Европе ресурс для IT-специалистов [Электронный ресурс] Режирм доступа: https://habr.com/company/microsoftlumia/blog/237545/ (дата обращения: 11.06.2018).

УДК 339.16.612.32:004

СИСТЕМЫ ВИБРАЦИОННОГО КОНТРОЛЯ И ДИАГНОСТИКИ

студент гр. 10306115 Куличик О.А.
Научный руководитель - к.т.н., доцент Гулай А.В.
Белорусский национальный технический университет
Минск, Беларусь

В современных условиях производственной деятельности, развитие систем вибрационного контроля и диагностики обусловлено необходимостью отслеживания состояния оборудования, агрегатов, ключевых узлов и механизмов, отказ которых может привести к финансовым, временным и другим потерям, что в целом оказывает негативное влияние на работу производства. Улучшению качества контроля и диагностики во многом способствует внедрение новых эффективных систем, методов и средств мониторинга.

Системы контроля и диагностики могут применяться в различных сферах производства. Следствием этого, возникает необходимость создания для каждого объекта или ответственного оборудования, производственной деятельности, уникальных систем вибрационного контроля и диагностики. Для таких объектов, рекомендуется использовать системы стационарного типа, которые традиционно включают в себя датчики измерения вибрации, измерительные и коммуникационные сервера сбора и обработки данных. Особенность данных систем – это возможность выявления технических изменений в режиме реального времени. Основными характеристиками таких систем являются: быстродействие, многокритериальность, пороговая адаптация и информационная точность.

Методы контроля и диагностики играют немаловажную роль в системах вибрационного контроля и диагностики. Одним из наиболее эффективных методов контроля технического состояния оборудования является мониторинг и анализ параметров вибрации. Благодаря этому методу, можно выявить дефект на этапе зарождения и спрогнозировать наступление критических изменений, когда оборудование должно быть выведено в ремонт. Это дает возможность заранее планировать выполнение ремонтных мероприятий, увеличить время непрерывной работы, сократить время восстановления работоспособности, повысить показатели технической готовности, использования и загрузки оборудования. Мониторинг вибрации может быть реализован двумя разным способами: периодическими виброобследованиями с использованием переносного оборудования или непрерывным сбором и обработкой данных с использованием стационарных автоматизированных систем вибромониторинга. Для определения состояния небольших установок, выполняющих некритичные функции, наиболее целесообразным является первый вариант [1].

Средства контроля и диагностики на сегодняшний день имеют достаточно большое разнообразие и применяются в различных сферах производственной деятельности. Измерительная техника, схожих характеристик, объединяется в группы: портативные приборы и системы диагностики, стационарные системы мониторинга и диагностики, мобильные (переносные) многоканальные системы мониторинга и диагностики [2].

При современных темпах развития промышленности, с появлением новых видов оборудования и технологий, необходимость в системах вибрационного контроля и диагностики неуклонно растёт. Использование данных систем приводит к снижению