Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

Кохновский
Станислав Игоревич

Использование сетей перестановок для улучшения статистических характеристик аппаратных генераторов случайных чисел

АВТОРЕФЕРАТ
диссертации на соискание степени магистра

по специальности 1-40 80 05 – Программная инженерия

Научный руководитель
Иванюк Александр Александрович
доктор технических наук,
профессор кафедры информатики

Минск 2023

ВВЕДЕНИЕ

Сфера применения аппаратных генераторов случайных последовательностей бит неимоверно велика: они используются в задачах моделирования, численного анализа, тестирования, криптографии и теории игр, но есть также и множество других весьма специфических областей применения.

В настоящее время существует множество разновидностей аппаратных генераторов случайных чисел, однако особое место в классификации занимают генераторы, логика работы которых основана на получении случайной последовательности из источников энтропии, которыми могут выступать различные физические явления (шумы, задержки и другие колеблющиеся показатели физических систем).

Однако не всегда реализации генераторов истинно случайных чисел генерируют действительно случайную последовательность, что может быть обусловлено влиянием множества факторов: внешней среды, внутренней структуры процесса или устройства, выбранного в качестве источника случайности, или изменением других показателей. Для оценки свойств генерируемой последовательности используются статистические наборы тестов, позволяющие заключить, насколько сильно показатели последовательности отличаются от статистических показателей истинно случайной последовательности.

Качественная генерация случайных чисел неимоверна важна для различных сфер, среди которых особо выделяются сфера защиты информационных систем. В последние годы наблюдается увеличение требований к статистическим свойствам генераторов случайных чисел. Стандартные реализации аппаратных генераторов случайных чисел могут не всегда обеспечивать требуемый уровень статистической случайности. Одним из способов улучшения статистических характеристик аппаратных генераторов случайных чисел является использование сетей перестановок.

В данной работе описан 32-битный генератор случайных чисел, для улучшения характеристик которого применяется метод перестановок бит в генерируемой последовательности с помощью сетей перестановок.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель данной диссертации состоит в исследовании и разработке генератора случайных чисел на основе ФНФ типа кольцевой осциллятор, а также методов, таких как использование сетей перестановок, для улучшения статистических характеристик спроектированного аппаратного генератора случайных чисел. В частности, будет проведен анализ и сравнение статистических характеристик разработанного генератора с использованием стандартных тестов на случайность. Также будет описано влияние различных параметров и конфигураций реализации на статистические свойства генератора, рассмотрены различные топологии сетей перестановок и исследовано их влияние на статистические свойства генератора случайных чисел.

Объектом исследования является аппаратный генератор случайных чисел, природа работы которого описывается ФНФ типа кольцевой осциллятор.

Предмет исследования - методы, модели и алгоритмы для повышения статистической случайности аппаратных генераторов случайных чисел, основой функционирования которых являются ФНФ на базе кольцевого осциллятора.

Публикации по теме исследования

Во время работы над диссертацией было произведено 6 докладов на научно-практических конференциях. Из них 2 тезиса опубликованы в сборнике материалов Международной научной конференции «Информационные технологии и системы» в 2020-2021 годах и 4 тезиса в сборниках 55, 56, 57, 58 научных конференций аспирантов, магистрантов и студентов БГУИР.

Также была защищена дипломная работа в рамках тематики данного исследования по теме «Алгоритмы синтеза проектных описаний цифровых устройств всевозможных перестановок».

СТРУКТУРА ДИССЕРТАЦИИ

Диссертация содержит следующие структурные части: общую характеристику работы, введение, четыре главы, заключение, список использованных источников, список публикаций соискателя и приложение.

В первой главе приводится понятийный аппарат в рамках тематики исследования, а также описывается метод генерации случайных чисел с использованием концепции физически неклонируемых функций.

Во второй главе описывается аппаратная часть системы проведения эксперимента, необходимые инструменты для реализации конфигурируемых частей системы. Также в данной главе содержится описание некоторых топологий перестановочных сетей, предложена авторская топология перестановочной сети и проанализированы её свойства.

Третья глава содержит описание процесса реализации и тестирования аппаратного генератора случайных чисел и вспомогательных компонентов, необходимых для проведения эксперимента.

В четвёртой главе приведены результаты экспериментов в различных режимах функционирования аппаратного генератора случайных чисел, произведено тестирование генератора и анализ результатов исследования.

ЗАКЛЮЧЕНИЕ

В рамках магистерской работы были рассмотрены различные подходы к реализации аппаратных генераторов случайных чисел. В качестве источника случайного процесса выбран кольцевой осциллятор с ячейкой памяти – D-триггером. Этот источник случайности основан на использовании уникальных параметров и характеристик кольцевых осцилляторов, что позволяет получить статистически случайные числа. Исследование различных параметров и конфигураций генератора позволило оптимизировать его статистические свойства и повысить эффективность генерации случайных чисел.

Характеристики генераторов истинно случайных чисел зависят от большого числа параметров, но значительное влияние на качество генерируемой последовательности оказывают особенности используемой для реализации аппаратуры, т. е. характеристики последовательностей бит, генерируемые различными аппаратными элементами, могут сильно отличаться. Особенностью реализации источника случайности на базе FPGA Nexys 4 производителя Diligent является появление большего количества единиц, чем нулей, в процессе генерации последовательности. В качестве средства нивелирования этого эффекта предложена постобработка генерируемой последовательности, для чего была разработана авторская перестановочная сеть на основе бета-элементов, описанных в топологиях баньяновских сетей, и проанализированы её свойства.

Для улучшения характеристик генерируемых последовательностей бит в работе предложено использование устройства всевозможных перестановок на основе авторской топологии перестановочной сети, осуществляющее постобработку сгенерированной последовательности из 32-битных слов. Для достижения лучших статистических показателей генератором случайных чисел на основе анализа свойств ключей устройства всевозможных перестановок был выбран метод генерации подходящих ключей.

В результате постобработки сгенерированной последовательности достигнуто улучшение статистических характеристик, что подтверждено результатами тестирования обработанной последовательности общепризнанным стандартом – набором статистических тестов NIST.

Среди направлений развития данной работы выделим поиск возможностей улучшения и оптимизации разработанного генератора, включая увеличение скорости генерации, расширение диапазона генерируемых чисел и адаптацию к специфическим требованиям конкретных приложений.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Кохновский, С. И. Методика проектирования комбинационного устройства всевозможных перестановок [Электронный ресурс] / С. И. Кохновский // Компьютерные системы и сети : сб. тезисов докладов. – БГУИР, Минск, 2019. – 287 с. – С. 205-207. – Режим доступа: https://www.bsuir.by/m/12_100229_1_136895.pdf. – Дата доступа: 22.03.2023.

2. Кохновский, С. И. Анализ аппаратурных затрат на реализацию цифрового устройства всевозможных перестановок [Электронный ресурс] / С. И. Кохновский // Компьютерные системы и сети: сб. тезисов докладов. – БГУИР, Минск, 2020. – 241 с. – С. 142-144. – Режим доступа: https://www.bsuir.by/m/12_100229_1_144999.pdf. – Дата доступа: 22.05.2023.

3. Кохновский, С. И., Иванюк А. А. Оценка ключей комбинационного устройства всевозможных перестановок [Электронный ресурс] / С. И. Кохновский, А. А. Иванюк // Информационные технологии и системы 2020 (ИТС 2020) : материалы международ. науч. конф. – Минск: БГУИР, 2020. – 235 с. – С. 105-106. – Режим доступа: https://its.bsuir.by/m/12_130111_1_147692.pdf. – Дата доступа: 05.04.2023.

4. Кохновский, С. И. Сглаживающие свойства ключей комбинационного устройства всевозможных перестановок [Электронный ресурс] / С. И. Кохновский // Компьютерные системы и сети: сб. тезисов докладов. – БГУИР, Минск, 2021. – 155 с. – С. 135-136. – Режим доступа: https://www.bsuir.by/m/12_100229_1_153926.pdf. – Дата доступа: 01.06.2023.

5. Кохновский, С. И., Иванюк А. А. Влияние длительности работы кольцевого осциллятора на статистические характеристики последовательности бит, сгенерированной аппаратным генератором случайных чисел [Электронный ресурс] / С. И. Кохновский, А. А. Иванюк // Информационные технологии и системы 2021 (ИТС 2021) : материалы международ. науч. конф. – Минск: БГУИР, 2021. – 248 с. – С. 126-127. – Режим доступа: https://its.bsuir.by/m/12_130111_1_157684.pdf. – Дата доступа: 05.06.2023.

6. Кохновский, С. И. Использование асинхронных D-триггеров для генерации уникальных цифровых идентификаторов [Электронный ресурс] / С. И. Кохновский // Компьютерные системы и сети: сб. тезисов докладов. – БГУИР, Минск, 2022. – 313 с. – С. 298-299. – Режим доступа: https://www.bsuir.by/m/12_100229_1_164084.pdf. – Дата доступа: 01.06.2023.