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

УДК 004.312

Кайкы Михаил Николаевич

Методы и средства генерирования случайных чисел с применением кольцевого осциллятора

АВТОРЕФЕРАТ
на соискание степени магистра
по специальности 7-06-0611-05 – Компьютерная инженерия

_____
(подпись магистранта)

Научный руководитель
Иванюк Александр Александрович
(фамилия, имя, отчество)
доктор техн.наук, проф.,
проф. каф. Информатики БГУИР
(ученая степень, ученое звание)

_____
(подпись научного руководителя)

Минск 2024

ВВЕДЕНИЕ

С целью повышения уровня безопасности современных интегральных схем (ИС), а также защиты от несанкционированного использования последних – применяются методы физической криптографии для получения неповторимых и уникальных последовательностей. Данные последовательности могут выступать как в роли идентификатора цифрового устройства, так и в качестве источника энтропии, например для генерации закрытых ключей в алгоритмах шифрования. Для получения описанных последовательностей современные методы физической криптографии применяют понятие физически неклонируемых функций (ФНФ). В силу изменения условий функционирования ИС (температуры окружающей среды, значений питающего напряжения), а также неизбежного износа и деградации кристалла последовательности, генерируемые с помощью ФНФ, являются нестабильными. ФНФ являются хорошим источником случайности для построения на их основе генераторов случайных числовых последовательностей, однако их вероятностные характеристики не всегда соответствуют криптографическим стандартам. В этой связи актуальной представляется задача синтеза аппаратных средств генерирования случайных числовых последовательностей на основе ФНФ с высокими характеристиками стабильности, уникальности, случайности, а также низкой уязвимостью к криптографическим атакам.

Отдельную нишу в разработке современных цифровых электронных устройств для генерации истинно случайных чисел занимают программируемые логические интегральные микросхемы (ПЛИС). Современные ПЛИС получили большое распространение как универсальные микросхемы для применения в качестве комплектующих в готовых изделиях, так и в качестве основы для стендов валидации при разработке современных систем на кристалле (СнК). Практическая применимость реализованных на ПЛИС типа FPGA генераторов истинно случайных чисел чрезвычайно широка. В области криптографии такие устройства могут служить источниками истинного случайного ключа для систем шифрования, обеспечивая высокий уровень защиты данных. В системах моделирования и симуляций генераторы позволяют получать высококачественные случайные последовательности, необходимые для статистического анализа и проверки алгоритмов. В области IoT и встроенных систем такие решения позволяют интегрировать надежные источники случайности непосредственно в аппаратные модули устройств, что существенно повышает безопасность и функциональность конечных продуктов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Актуальность темы диссертационной работы обусловлена растущей потребностью в обеспечении высокой степени информационной безопасности в современных цифровых системах и устройствах. В условиях активного распространения киберугроз, роста объемов передаваемых и хранимых данных, а также увеличения требований к надежности криптографических средств, особое значение приобретает создание устойчивых и качественных источников истинно случайных чисел. Современные стандарты и нормативные документы, такие как NIST SP 800-90 серии и техническая спецификация ТС 26.4.001-2019, регламентируют требования к качеству, надежности и криптографической стойкости генераторов случайных чисел. В этих документах подчеркивается важность использования физических источников энтропии, таких как физически неклонируемые функции (ФНФ), реализуемые на базе характеристик микросхем и элементов памяти, а также кольцевых осцилляторов и бистабильных элементов. В связи с этим актуальна задача разработки методов и средств получения неповторимых, устойчивых и статистически качественных случайных последовательностей, а также их практической реализации в аппаратных платформах. Особую актуальность приобретает использование программируемых логических интегральных схем (ПЛИС) для реализации физических источников энтропии. Это обусловлено их универсальностью, возможностью быстрого прототипирования, а также возможностью интеграции в современные системы с ограниченными требованиями к размеру и энергопотреблению. Важно подчеркнуть, что разработка методов управления метастабильностью, моделирования поведения бистабильных элементов памяти и кольцевых осцилляторов, а также создание архитектур генераторов случайных чисел на базе ПЛИС непосредственно способствует повышению уровня их криптостойкости и эффективности. Кроме того, актуальность темы связана с необходимостью повышения устойчивости генераторов к внешним воздействиям, вариациям условий эксплуатации и технологическим отклонениям, что особенно важно для систем IoT, встроенных устройств и доверенных приложений, где требования к безопасности и надежности крайне высоки. Внедрение новых методов синтеза и моделирования физических источников энтропии позволяет обеспечить соответствие международным стандартам, повысить качество генерируемых последовательностей и расширить их применение в различных областях информационной безопасности и цифровых технологий.

Цели и задачи исследования

Целью исследования являются методы и средства генерации истинно случайных чисел на основе кольцевых осцилляторов и бистабильных элементов памяти с использованием программируемых логических интегральных схем (ПЛИС), обеспечивающих высокие показатели энтропии,

и соответствие международным криптографическим стандартам (NIST SP 800-90, ТС 26.4.001-2019).

К задачам исследования относятся:

1. Исследование требований NIST SP 800-90 (A, B, C) и ТС 26.4.001-2019 к генераторам случайных чисел.
2. Анализ статистических тестов (Health Tests, NIST STS) для оценки качества случайных последовательностей.
3. Исследование физически неклонируемых функций (ФНФ) как источников случайных чисел.
4. Сравнение характеристик ФНФ типа SRAM и Арбитр на базе ПЛИС и промышленных ИС, оценка их стабильности, уникальности и случайности выходных последовательностей.
5. Создание аналитической модели бистабильного элемента памяти.
6. Моделирование конфигурируемых кольцевых осцилляторов.
7. Разработка архитектуры ГИСЧ с блоком управления источником энтропии и детектором энтропии на базе ПЛИС.
8. Экспериментальная оценка характеристик ГИСЧ.
9. Проведение статистических тестов (NIST STS) для проверки случайности последовательностей.

Степень разработанности проблемы

Степень разработанности проблемы генерации истинных случайных чисел в мире является высокой и активно исследуемой. В последние годы значительно продвинулся научный и практический уровень в области физически источников энтропии, таких как физически неклонируемые функции (ФНФ), кольцевые осцилляторы и бистабильные элементы памяти. В области реализации активно применяются ПЛИС, микросхемы SRAM, кольцевые осцилляторы и другие физические источники энтропии. В научных публикациях и прикладных разработках широко исследуются методы моделирования, анализа и тестирования таких источников, что позволяет создавать более надежные и устойчивые к внешним воздействиям генераторы. Однако, вопросы повышения стабильности, защиты от атак и интеграции в современные системы остаются актуальными и требуют дальнейших исследований.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 7-06-0611-05 Компьютерная инженерия.

Теоретическая и методологическая основа исследования

В основу диссертации легли работы отечественных и зарубежных учёных в области исследования, разработки и работы генераторов истинно

случайных чисел на базе ПЛИС и микроконтроллеров с использованием структур типа физически неклонируемая функция.

Информационная база исследования сформирована на основе литературы, открытой информации, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна, теоретическая и практическая значимость

Научная новизна исследования заключается в разработке новых методов моделирования и оценки физически источников энтропии, таких как кольцевые осцилляторы и бистабильные элементы памяти. В рамках работы предложен метод управления метастабильностью бистабильных элементов памяти для извлечения случайности, разработана аналитическая модель бистабильного элемента памяти, экспериментально доказана возможность применения ФНФ на основе SRAM в качестве источников случайности.

Теоретическая значимость состоит в расширении существующих моделей генераторов случайных чисел, что способствует более глубокому пониманию процессов генерации и повышения надежности криптографических систем.

Практическая ценность проявляется в создании методов проектирования и тестирования физических генераторов, используемых в современных информационных системах. Внедрение результатов исследования способствует совершенствованию стандартов и практических решений в области генерации истинных случайных чисел.

Основные положения, выносимые на защиту

1. Предложена аналитическая модель бистабильного элемента памяти как источника случайности, на модели доказано, что бистабильный элемент памяти способен переходить в состояние автоколебаний и может быть использован для дальнейшей генерации истинно случайных чисел в цифровых системах.
2. Предложена новая структура генератора истинно случайных чисел, с введением блока управления источником случайности. Экспериментально доказано что статистические характеристики предложенного генератора соответствуют характеристикам случайных последовательностей с высоким уровнем энтропии и способны повышать его в диапазоне от 0.4 до 0.9999.
3. Доказано что, ячейки памяти типа SRAM соответствуют предложенной аналитической модели бистабильного элемента и на практике могут быть использованы в качестве источников случайности для использования в генераторе истинно случайного числа.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Актуальность темы диссертационного исследования обусловлена возрастающими требованиями к информационной безопасности в условиях массовой цифровизации и распространения интернета вещей. Генерация истинно случайных чисел играет ключевую роль в криптографических системах, обеспечивая создание уникальных идентификаторов и защищённых ключей шифрования.

В первой главе проведён анализ современных стандартов проектирования генераторов случайных чисел. Особое внимание уделено серии рекомендаций NIST SP 800-90, которые устанавливают строгие требования к детерминированным и физическим генераторам. Исследование показало, что стандарт NIST SP 800-90B, посвящённый оценке энтропии, является наиболее критичным для аппаратных реализаций.

Вторая глава посвящена исследованию физически неклонируемых функций как источников энтропии. Экспериментальное исследование структуры ФНФ типа Арбитр на базе ПЛИС Artix-7 продемонстрировало их высокую надёжность, но выявило проблему неравномерного распределения ответов ФНФ. Более перспективными оказались ФНФ на основе статической памяти (SRAM), которые показали близкое к идеальному соотношение нулей и единиц. Однако детальный анализ промышленных образцов микросхем памяти Microchip 23K256 выявил их чувствительность к колебаниям питающего напряжения, что требует дополнительных исследований и разработки специальных методов стабилизации ответов.

Третья глава содержит разработку нового метода синтеза генераторов случайных последовательностей. Предложена аналитическая модель бистабильного элемента памяти, описывающая его поведение в различных режимах работы, включая состояние метастабильности. Моделирование с использованием языка описания аппаратуры SystemVerilog подтвердило возможность управления процессом генерации случайных данных путём целенаправленного перевода элемента в режим автоколебаний. Особое внимание уделено исследованию конфигурируемых кольцевых осцилляторов, чья частота колебаний может регулироваться путём изменения управляющих параметров.

В четвёртой главе представлена практическая реализация генератора истинно случайных чисел на базе ПЛИС. Разработанная архитектура включает блок управления источником энтропии, источник энтропии на базе бистабильного элемента памяти и конфигурируемых кольцевых осцилляторов, блок обнаружения энтропии и регистр случайных чисел.

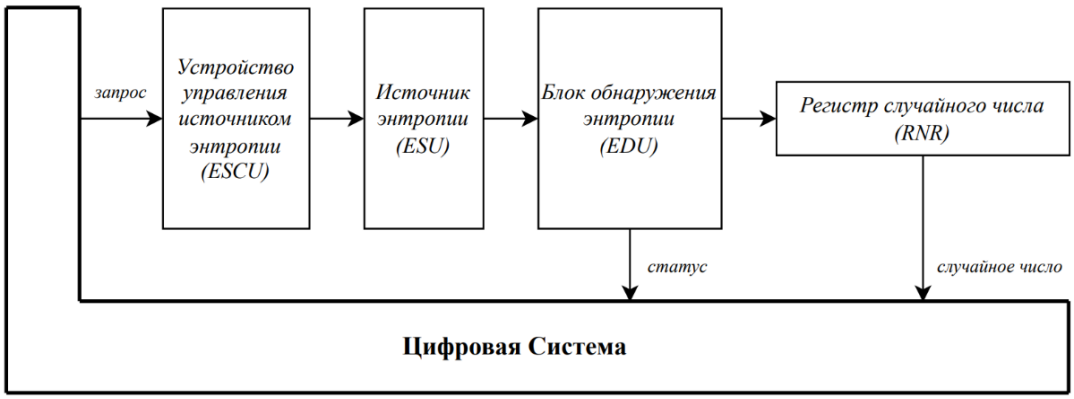

Рисунок 1. – Усовершенствованная схема генератора истинно случайных последовательностей

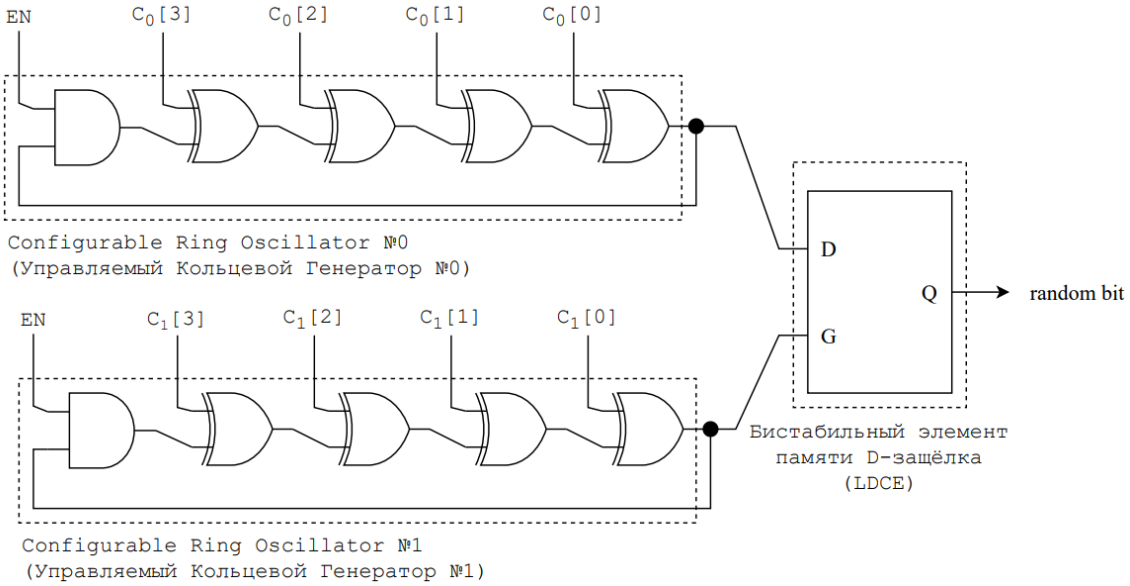

Рисунок 2. – Схема источника энтропии в генераторе истинно случайных последовательностей

Экспериментальные исследования показали, что уровень энтропии по Шеннону достигает значения 0,999 при оптимальных параметрах работы системы. Результаты тестирования с использованием набора NIST STS подтвердили соответствие большинству критериев случайности, хотя некоторые тесты (Frequency, Run) требуют дополнительной постобработки генерируемых последовательностей.

ЗАКЛЮЧЕНИЕ

Данная работа посвящена разработке методов и средств генерации истинно случайных чисел на основе цифровых схем. В рамках работы проведен комплексный анализ существующих стандартов и методик проектирования генераторов случайных последовательностей, таких как стандарты NIST SP 800-90 серии и спецификация ТС 26.4.001-2019, что позволило сформировать требования к качеству, надежности и криптостойкости современных источников случайности. Особое внимание в работе уделено изучению физических источников энтропии, реализуемых на базе физически неклонируемых функций, таких как SRAM-память, кольцевые осцилляторы, бистабильные элементы памяти, реализованные на программируемых логических интегральных схемах и промышленных микросхемах.

Доказано, что уникальные вариации, обусловленные технологическими параметрами производства интегральных схем, позволяют получать неповторимые, неклонируемые и статистически качественные исходные данные для генерации случайных чисел. Проведен экспериментальный анализ стабильности, уникальности и случайности векторов, сформированных на базе ФНФ, и выявлены основные ограничения и возможности использования таких источников в условиях изменения внешних факторов, включая вариации питающего напряжения. В рамках исследования предложен новый метод синтеза генераторов случайных последовательностей с использованием конфигурируемых кольцевых осцилляторов и бистабильных элементов памяти. Разработана аналитическая модель бистабильного элемента, которая позволяет оптимизировать параметры устройств для повышения уровня энтропии и управляемого перехода в режим автоколебаний, используемый для формирования случайных бит.

Разработана архитектура ГИСЧ с блоком управления источником энтропии, детектором энтропии и блоками постобработки, что обеспечивает высокий уровень надежности и криптостойкости цепочки. Проведено моделирование и тестирование разработанных решений в реальных условиях, выполнена оценка их характеристик с помощью современных стандартных статистических тестов, таких как NIST SP 800-22. Полученные результаты подтвердили высокое качество сгенерированных последовательностей, их соответствие требованиям статистической случайности.

Полученные результаты демонстрируют перспективность использования физических и цифровых элементов памяти в качестве надежных источников энтропии для генераторов истинных случайных чисел, а также их возможности для внедрения в системы IoT и другие доверенные устройства.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1. Кайкы, М. Н. Исследование стабильности промышленной SRAM памяти, используемой для неклонируемой идентификации / М. Н. Кайкы, А. А. Иванюк // Информационные технологии и системы 2022 (ИТС 2022) = Information Technologies and Systems 2022 (ITS 2022) : материалы Международной научной конференции, Минск, 23 ноября 2022 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2022. – С.79–80.
2. Кайкы М. Н. Применимость и сравнение ФНФ типа Арбитр и статической памяти в системах идентификации / М. Н. Кайкы, А. А. Иванюк. — Текст : электронный // Молодежь и наука : материалы международной научно-практической конференции старшеклассников, студентов и аспирантов (27 мая 2022 г.) : в 2 томах. — Нижний Тагил : НТИ (филиал) УрФУ, 2022. — Том 1. — С. 257-259.
3. Кайкы, М. Идентификация цифровых устройств с помощью бистабильных элементов, реализованных на FPGA = Identification of digital devices using bistable elements implemented on FPGA / Кайкы М. // Компьютерные системы и сети : сборник статей 58-й научной конференции аспирантов, магистрантов и студентов, Минск, 18–22 апреля 2022 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2022. – С. 186–191.
4. Кайкы, М. Н. Сравнение характеристик ФНФ статической памяти с использованием плис и промышленных микросхем = Comparison of static memory puf characteristics using FPGA and industrial Ics / М. Н. Кайкы, А. А. Иванюк // Приборостроение-2022 : материалы 15-й Международной научно-технической конференции, 16-18 ноября 2022 года, Минск, Республика Беларусь / редкол.: О. К. Гусев (председатель) [и др.]. – Минск : БНТУ, 2022. – С. 37-39.
5. Кайкы, М. Н. Исследование характеристик физически неклонируемых функций, построенных на базе комбинированного генератора = Investigation of the characteristics of a physically unclonable function built on the basis of a combined generator / М. Н. Кайкы // Компьютерные системы и сети : сборник статей 59-й научной конференции аспирантов, магистрантов и студентов, Минск, 17–21 апреля 2023 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2023. – С. 80–86.
6. Шамына, А. Ю. Программно-аппаратный комплекс для быстрого прототипирования и исследования криптографических примитивов на базе ПЛИС / А. Ю. Шамына, М. Н. Кайкы, А. А. Иванюк // Информационные технологии и системы 2023 (ИТС 2023) = Information Technologies and Systems 2023 (ITS 2023) : материалы Международной научной конференции, Минск, 22 ноября 2023 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2023. – С. 117–118.

7. Kaiky, M. Fast prototyping of reconfiguable true random number generation ip-core / M. Kaiky, A. Shamyna, A. Ivaniuk // Информационные технологии и системы 2023 (ИТС 2023) = Information Technologies and Systems 2023 (ITS 2023) : материалы Международной научной конференции, Минск, 22 ноября 2023 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2023. – С. 125–126.

8. Burko, L. Health tests hardware implementation for entropy sources / L. Burko, M. Kaiky, A. Ivaniuk // Информационные технологии и системы 2023 (ИТС 2023) = Information Technologies and Systems 2023 (ITS 2023) : материалы Международной научной конференции, Минск, 22 ноября 2023 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2023. – С. 119–120.

9. Kaiky, M. Random number generation on reconfigurable ring oscillator / M. Kaiky, A. Ivaniuk // Информационные технологии и системы 2023 (ИТС 2023) = Information Technologies and Systems 2023 (ITS 2023) : материалы Международной научной конференции, Минск, 22 ноября 2023 / Белорусский государственный университет информатики и радиоэлектроники ; редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2023. – С. 123–124.

10. Кайкы, М. Н. Источник энтропии на базе конфигурируемых кольцевых осцилляторов = Source of entropy based on configurable ring oscillators / М. Н. Кайкы, А. А. Иванюк // III Республиканский форум молодых ученых учреждений высшего образования : сборник материалов форума, Брест, 21–24 мая 2024 г. / Министерство образования Республики Беларусь, Брестский государственный технический университет, Брестский государственный университет имени А. С. Пушкина ; редкол.: Н. Н. Шалобыта (гл. ред.) [и др.]. – Брест : БрГТУ, 2024. – С. 34–35.