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

УДК 004.312

Петровский
Дмитрий Алексеевич

АППАРАТНО-ПРОГРАММНАЯ МОДИФИКАЦИЯ ЯДРА RISC-V I32 С ЦЕЛЬЮ УВЕЛИЧЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ ДЛЯ ЗАДАННОГО АЛГОРИТМА

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 2025

ВВЕДЕНИЕ

Современные вычислительные системы требуют высокой эффективности и универсальности процессорных архитектур, способных обеспечивать выполнение разнообразных задач в условиях постоянного роста требований к скорости, надежности и безопасности. Одной из наиболее перспективных и гибких решений в этой области является архитектура RISC - V – открытая, модульная и легко расширяемая архитектура команд, которая за короткое время получила широкое распространение среди ведущих технологических компаний и исследовательских институтов. Благодаря своей открытой спецификации, возможности кастомизации наборов команд и низкой стоимости лицензирования, RISC-V становится универсальной платформой для создания современных решений в области встроенных систем, интернета вещей, высокопроизводительных вычислений и, что особенно актуально, криптографической защиты и информационной безопасности.

Особое значение в криптографических системах имеет генерация случайных чисел, являющаяся основой формирования секретных ключей и криптографических протоколов. Высококачественные источники случайных чисел должны обеспечивать непредсказуемость и равномерность распределения, что важно для предотвращения крипто аналитических атак. В современных системах используются как псевдослучайные числа (ПСЧ), основанные на математических алгоритмах, так и истинно случайные числа (ИСЧ), полученные из физических источников энтропии, таких как радиоактивный распад, фазовое дрожание и т.д.

Генерация случайных чисел тесно связаны с аппаратной реализацией ГИСЧ и требуют специальных методов и алгоритмов для повышения их статистических характеристик. В этом контексте архитектура RISC-V обладает значительным потенциалом для интеграции модулей постобработки случайных чисел непосредственно в вычислительную платформу.

Стандарты, такие как рекомендации Национального института стандартов и технологий США (NIST), определяют требования к источникам энтропии и методам проверки качества случайных чисел. В этих документах подчеркивается необходимость использования схем постобработки для повышения статистических характеристик, особенно при работе с источниками, не обладающими полной энтропией. В рамках исследования предполагается изучение архитектуры RISC-V и подхода по интеграции расширений, что позволит обеспечить выполнение требований криптографической безопасности при минимальных накладных расходах.

ОБЩАЯ ХАРАКТЕРИТСИКА РАБОТЫ

Актуальность темы диссертации

Актуальность работы обусловлена необходимостью повышения производительности и надежности процессорных решений, предназначенных для криптографической обработки и генерации случайных чисел. В рамках магистерской диссертации предполагается разработка программно-аппаратных модификаций ядра архитектуры RISC-V, направленной на интеграцию предложенного метода постобработки, анализ его статистических характеристик, производительности и сравнение с аналогичными разработками.

Таким образом, выполненная работа внесет вклад в развитие технологий безопасных вычислительных систем на базе открытых архитектур, способных отвечать современным требованиям к скорости, надежности и криптографической стойкости. Исследование также откроет новые направления в интеграции методов обработки случайных чисел в процессорные платформы, что важно для повышения уровня информационной безопасности в различных областях — от встроенных систем и интернета вещей до высокопроизводительных вычислительных комплексов.

Цели и задачи исследования

Цель работы является разработка аппаратно-программной модификации ядра процессора архитектуры RISC-V для повышения производительности алгоритма постобработки случайных чисел. Для достижения данной цели необходимо решить следующие задачи:

1. Исследование отрытой архитектуры набора команд RISC-V и методов постобработки случайных чисел;
2. Разработка метода постобработки случайных чисел, с целью улучшения характеристик генерируемых последовательностей, на базе алгоритма многоканального сигнатурного анализатора;
3. Создание аппаратно-программной модификации ядра RISC-V для повышения производительности алгоритма постобработки случайных чисел, на основе предложенного метода;
4. Экспериментальная оценка характеристик выходных последовательностей предложенного алгоритма постобработки;
5. Оценка аппаратных затрат ПЛИС для реализации ядра RISC-V I32 с предложенной аппаратно-программной модификацией;
6. Оценка производительности алгоритма постобработки случайных чисел.

Объект и предмет исследования

Объектом исследования является процессорная архитектура RISC-V. Предмет исследования – алгоритмы постобработки случайных чисел.

Область исследования

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

Методология и методы проведенного исследования

Решение рассматриваемых в диссертации задач базируется на общенаучных методах, таких как структурный и сравнительный анализ, а также метод формализации. Кроме того, в работе используется системный подход к анализу и разработке алгоритмов постобработки случайных чисел.

Научная новизна

1. Предложен алгоритм постобработки случайных числен основанный на применении многоканального сигнатурного анализатора, реализующего сжатие исходных данных, как в пространстве, так и во времени, с целью улучшения характеристик генерируемых выходных последовательностей;
2. Экспериментальным путем была показана возможность конфигурации предложенного алгоритма постобработки случайных чисел, с целью улучшения характеристик генерируемых выходных последовательностей;
3. На основе предложенного алгоритма было реализовано расширение инструкций ядра RISC-V, с целью повышения производительности предложенного алгоритма постобработки случайных чисел.

Положения, выносимые на защиту

1. Алгоритм постобработки случайных чисел, основанный на применении многоканального сигнатурного анализатора, реализующего сжатие исходных данных, как в пространстве, так и во времени, с целью улучшения характеристик генерируемых выходных последовательностей, позволяющий достичь уровня информационной энтропии по Шеннону 0,99985;

2. Аппаратно-программная модификация ядра RISC-V с интеграцией двух инструкций, позволяющая повысить производительность предложенного алгоритма постобработки случайных чисел в сравнении с программной реализацией в 99 раз и требующая меньших аппаратных затрат в сравнении со стандартными расширениями.

Личный вклад магистранта

Результаты, приведенные в диссертации, получены соискателем лично. Вклад научного руководителя, доктора технических наук, профессора Иванюка А.А. связан с постановкой цели и задач исследования, определением возможных путей решения и обсуждением результатов исследований, проводимых автором. В публикациях с соавторами вклад соискателя определяется рамками излагаемых в диссертации результатов.

Апробация диссертации и информации об использовании её результатов

Основные результаты диссертационной работы докладывались и обсуждались на 3 международных и республиканских научных конференциях:

Научной конференции аспирантов, магистрантов и студентов БГУИР (60-я) – Минск, Беларусь, 2024; Международной научно-технической конференции «Информационные технологии и системы» (ITS) – Минск, Беларусь, 2023, 2024.

Научная статья «Схема постобработки случайных чисел на базе многовходового регистра сдвига» подготовлена и отправлена в редакцию журнала Доклады БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Актуальность темы диссертационного исследования обусловлена ростом требований к производительности и безопасности вычислительных систем, основанных процессорных архитектурах. Постобработка случайных чисел, позволяет повысить характеристик генерируемых последовательностей, такие как случайность, равномерность распределения и т.д., которые играют ключевую роль в криптографических приложениях, повышающих безопасность системы.

В первой главе дан детальный анализ архитектуры процессора RISC-V и подходов к постобработке случайных чисел. Особое внимание уделено рекомендациям NIST SP 800-90B, которые определяют требования к характеристикам алгоритмов и рекомендует проверенные схемы постобработки случайных числе. Так же были проанализированы алгоритм постобработки на основе регистра сдвига с линейной обратной связью (англ. LFSR). Исследование показало, что архитектура RISC-V отличается высокой модульностью, а алгоритмы, рекомендованные NITS, могут быт интегрированы с использованием стандартных расширений.

Во второй главе предлагается метод постобработки случайных чисел, основанный на принципе зажатия данных в пространстве и во времени с потерями, на базе алгоритма функционирования многоканального сигнатурного анализатора. Разработан программный алгоритм постобработки случайных чисел с учетом особенностей архитектуры RISC-V и оптимизацией расчета коэффициентов алгоритма. Оптимизация позволила заменить возведением матриц, коэффициентов обратной связи и сдвига, вычислением элементов псевдослучайных последовательностей используя алгоритм функционирования LFSR по схеме Галуа и Фибоначчи.

Предложено расширение набора инструкций ядра RISC-V, для повышения производительности алгоритма сжатия данных. Которое заключается в добавлении двух команд (см. таблицу 1) для расчета состояния LFSR по схеме Галуа и Фибоначчи. Где операнды *rs*1 и *rs*2 это текущее состояние LFSR и коэффициенты порождающего полинома. Результат команды *rd* – следующее состояние LFSR.

Таблица 1 – Описание предлагаемых команд

OP	*Funct*3	*Funct*7	Тип	Инструкция	Описание
01010	000	-	*Custom*-1	*lfsrf rd*, *rs*1, *rs*2	Команда вычисляет состояние *LFSR* по схеме Фибоначчи.
01010	001	-	*Custom*-1	*lfsrg rd*, *rs*1, *rs*2	Команда вычисляет состояние *LFSR* по схеме Галуа.

В листинге 1.а представлен фрагмент микропрограммы предложенного алгоритма без использования модификации, полужирным выделены фрагмент, который будет заменен. В листинге 1.б представлен этот же фрагмент, но с использованием предложенных команд.

Листинг 1 – Фрагмент микропрограммы предложенного алгоритма а) без использования модификации б) с использованием модификации

а)

```
A_LOOP:
    BGE t0, a1, B_START
    LW t4, 0(a4)
    ADDI a4, a4, 0x4

FDB_F:
    XOR t1, s0, t4
    SRL t2, a1, 1

FDB_F_LOOP:
    BNE t2, zero, FDB_F_END
    SRL t3, t1, t2
    XOR t1, t1, t3
    SRL t2, t2, 1
    JAL zero, FDB_F_LOOP
FDB_F_END:
    ADDI s2, t2, 0
    SLL t2, t2, 1
    OR s2, s2, t2
    ADDI t0, t0, 1
    JAL zero, A_LOOP
```

б)

```
A_LOOP:
    BGE t0, a1, B_START
    LW t4, 0(a4)
    ADDI a4, a4, 0x4

FDB_F:
    LFSRF s2, s0, t4
    ADDI t0, t0, 1
    JAL zero, A_LOOP
```

Данные команды позволяют сократить объем микропрограммы на 25% от исходного объема, что в свою очередь снижает требования к памяти и повышает производительность алгоритма.

Также разработано собственное ядро процессора на архитектуре RV32I с использованием языка описания аппаратуры Verilog, оснащенное пятиступенчатым конвейером и блоком управления конфликтами. В которое произведена интеграция предложенного расширения набора команд.

В третей главе выполнена практическая апробация предложенного алгоритма постобработки случайных чисел с использованием разработанного универсального программного стенда для моделирования и тестирования. Для

анализа использовались скрипты на Python, статистические тесты NIST 800-22, а также различные наборы входных данных.

Проведен комплексный статистический анализ – расчет энтропии, построение гистограмм, автоматизированное тестирование, что подтвердило высокое качество и равномерность распределения выходных последовательностей. Особое внимание уделено оценке влияния параметров алгоритма (порождающих полиномов, коэффициентов сжатия, разрядности входных слов и внутреннего состояния). Была выполнена серия экспериментов, показавших, что использование примитивных полиномов и оптимальных коэффициентов дает стабильные и высокие статистические характеристики, соответствующие требованиям криптографической надежности. Произведено сравнение предложенного алгоритма с классическими схемами (SHA-1, SISR, другие), в результате которого выявлено, что предложенный алгоритм по качеству статистических характеристик выходных последовательностей не уступает классическим решениям и показывает высокие результаты по тестам NIST.

Произведен анализ аппаратных затрат ПЛИС разработанного ядра RV32I с предложенной модификацией при имплементации в кристалл XC7Z010. Выполнено сравнение аппаратных затрат с ядром RV32I Zkn, где имплементировано расширения позволяющее ускорить криптографические функции, используемые для постобработки по рекомендациям NIST.

Таблица 1 – Аппаратные затраты ПЛИС при размещении RV32I

Расширение	*LUTs*	*FFs*	*MUXs*	*Block RAMs*
Предложенная реализация *RV32I*				
Отсутствует	1429	1433	256	1
lfsr	1500	1433	256	1
Различие	**71**	**0**	**0**	**0**
Референсная реализация *RV32I*[1]				
Отсутствует	1353	1035	278	1
Zkn	2935	1138	278	1
Различие	**1582**	**103**	**0**	**0**

Представлен анализ производительности предложенного алгоритма на собственном процессорном ядре с использованием модификации и без неё. Было произведено сравнение производительности предложенного решения алгоритмом HMAC(SHA-2) на ядре RV32I Zkn.

[1] Процессорное ядро RISC-V с набором базовых расширений архитектуры. Проект с отрытым исходным кодом доступен по ссылке https://github.com/secworks/cmac (дата обращения: 06.05.2025)

ЗАКЛЮЧЕНИЕ

На основании проведенного комплексного анализа и серии исследований можно сделать вывод о том, что архитектурная основа RISC-V представляет собой модульную и адаптивную платформу, обладающую значительным потенциалом для интеграции современных расширений.

Благодаря этим модификациям платформа способна обеспечивать выполнение алгоритмов в том числе постобработки случайных чисел, полностью удовлетворяющих рекомендациям, принятым в NIST. Алгоритмы на основе криптографических функций характеризуются высокой статистической надежностью и устойчивостью к случайным вариациям, в то время как использование генераторов линейного сдвига с обратной связью (*LFSR*) способствует снижению аппаратных и временных затрат, необходимых для качественной обработки данных.

Разработанная аппаратно-программная адаптация схемы MISR*, реализованная на базе архитектуры RISC-V, позволила существенно повысить эффективность постобработки случайных чисел. В процессе проектирования и реализации данного решения были внедрены схемы расчета обратной связи *LFSR* посредством модификации АЛУ. В следствии чего были добавлены дополнительные команды в качестве расширения для RVI32.

Результаты экспериментов показали, что этот подход обеспечивает не только простоту и надежность внедрения, но и минимальное влияние на существующую архитектуру системы, что подтверждает высокую стабильность функционирования и существенное увеличение вычислительной производительности. Подтверждением эффективности разработанной схемы стали экспериментальные данные, полученные при проведении испытаний с использованием разных наборов данных, что демонстрирует высокую стабильность работы MISR* в различных условиях.

Выполненные тесты, проведенные в соответствии с методиками NIST, показали, что качество сгенерированных случайных чисел является статистически значимым и соответствует современным стандартам криптографической защиты.

Полученные экспериментальные и аналитические результаты аргументированно демонстрируют потенциал использования данных решений в практических системах, где критически важны высокая вычислительная эффективность, минимальные затраты аппаратных ресурсов и строгие требования по безопасности генерации случайных чисел, что обеспечивает дальнейшую интеграцию разработанных технологий в современные системы обработки информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

[1] RISC-V hardware modification for M-sequences generation - стр. 127-128 Petrovsky D., Ivaniuk A. Information Tehnologies and Systems 2023 (ITS 2023) : материалы международной научной конференции, Минск, Беларусь, 22 ноября / Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2023

[2] Петровский, Д. А. Схема постобработки цифровой последовательности случайных чисел / Д. А. Петровский // Компьютерные системы и сети : сборник статей 60-й научной конференции аспирантов, магистрантов и студентов, Минск, 22–26 апреля 2024 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2024. – С. 729–730.

[3] Петровский, Д. А. Анализ характеристик схемы постобработки последовательности случайных чисел на основе многоканального сигнатурного анализатора / Д. А. Петровский, А. А. Иванюк // Информационные технологии и системы 2024 (ИТС 2024) = Information Technologies and Systems 2024 (ITS 2024) : материалы международной научной конференции, Минск, 20 ноября 2024 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2024. – С. 93–94.