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

УДК 004.272

Ероховец
Влада Андреевна

Процессор SHA-3 на базе FPGA

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-40 80 01 «Компьютерная инженерия»

Научный руководитель
Станкевич Андрей Владимирович
доцент, кандидат технических наук

Минск 2022

ВВЕДЕНИЕ

Формирование уникального идентификатора для всех видов документов – одна из основных задач хеширования. С его помощью сообщения произвольной длины идентифицируются уникальной последовательностью символов для дальнейшего использования. Данное свойство может быть использовано в большом разнообразии систем. Среди них: банковская сфера, где необходимо быть точно уверенным в уникальности документа и правильности проведённого платежа; сетей интернет, где по трафику можно определить, не изменён ли он был где-то посредине и множестве других сфер.

Один из самых широко используемых алгоритмов SHA-2 в настоящее время признан уязвимым к атакам, хоть и не был полностью взломан. На смену ему пришёл стандарт SHA-3, привнёсший большое количество идей для формирования хеш-значения сообщения.

Программные реализации стандарта несомненно более гибкие в плане использования, однако их дальнейшее улучшение упирается в возможности аппаратной платформы. Использование в данном случае FPGA позволит продвинуться дальше в процессе модернизации описаний.

В текущей работе рассмотрены алгоритмы хеширования и указаны причины смены стандарта, рассмотрены основные схемы реализации стандарта и переход от одной архитектуры к другой, выделены основные плюсы и минусы каждой реализации, проведено сравнение с существующими реализациями.

Основными задачами работы являются анализ алгоритмов и их существующих реализаций, а также реализации собственных структур, позволяющих обрабатывать сообщения произвольной длины.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель данной работы: разработка оптимального с точки зрения производительности и аппаратных затрат устройства формирования хеш-значения сообщения на базе ПЛИС.

Задачи исследования: анализ аппаратных реализаций стандарта хеширования SHA-3, максимизация производительности, оптимизация расхода аппаратных ресурсов.

Объект исследования: алгоритмы генерации хеш-значения семейств SHA-2 и SHA-3, архитектурные решения устройства для его формирования.

Предмет исследования: аппаратные реализации стандартов хеширования.

Личный вклад автора выражен в самостоятельном исследовании:

– анализ стандартов и алгоритмов хеширования семейства SHA-2 и SHA-3;

– сравнительный анализ существующих аппаратных реализаций на основе семейства алгоритмов хеширования SHA-3;

– анализ алгоритма хеширования SHA-3-256 и его внутренних алгоритмов с целью максимизации производительности и минимизации аппаратных затрат;

– исследование аппаратных затрат и производительности реализации стандарта хеширования.

Результатом произведенного анализа, расчетов и оптимизации явилась разработка собственных устройств формирования хеш-значений сообщений произвольной длины на основе стандарта FIPS 202.

Практическая значимость результатов диссертации состоит в разработке нескольких вариантов устройств для формирования хеш-значения, которые отличаются по строению и своим характеристикам.

Материалы диссертации докладывались на 57-й и 58-й научных конференциях аспирантов, магистрантов и студентов БГУИР.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Существующие алгоритмы имеют широкую область применения, в связи с чем происходит постоянное усложнение алгоритмов для обеспечения их криптостойкости. Рассматриваемые семейства алгоритмов SHA-2 и SHA-3 в разное время являлись национальными стандартами США. Целью работы являлась реализация алгоритма SHA-3 на базе FPGA.

Для успешного выполнения цели были выделены следующие основные задачи работы:

1. Провести анализ алгоритмов хеширования семейства SHA и выделить основные отличия новых версий от предыдущих.
2. Провести анализ алгоритма стандарта FIPS 202 с точки зрения особенностей его реализации на базе ПЛИС с целью минимизации аппаратных затрат и максимизации производительности.
3. Провести исследования возможных архитектур аппаратного описания специализированного процессора.
4. Реализовать предложенные архитектурные решения на базе FPGA семейства Virtex-7 Xilinx.
5. Исследовать аппаратные затраты и производительность разработанных специализированных процессоров. Оценить применение каждой архитектуры.

В главе 1 проведён сравнительный анализ алгоритмов хеширования семейства SHA-2 и SHA-3. Показаны введённые в алгоритмах SHA-2 структура Меркла-Дамгора, пояснена схема её работы. Описаны основные алгоритмы, входящие в состав. Рассмотрено семейство алгоритмов SHA-3. Описаны его внутренние функции. Показан путь развития алгоритмов от семейства SHA-2 к SHA-3, показаны узкие места стандарта SHA-2 и причины его замены на более новый стандарт.

Описывается и детально разбирается нововведение алгоритмов семейства SHA – криптографическая губка. Проводится анализ её фаз, описываются возможные вариации использования структуры. Показан процесс формирования векторов для их использования во внутреннем алгоритме перемешивания – Keccak.

Рассматриваются также алгоритмы, входящие в состав алгоритма SHA-3-256, такие как Keccak и алгоритмы раундовых функций. Проведён их анализ, а также предложены некоторые улучшения. Описываются все процессы, происходящие внутри каждого алгоритма. Подробно рассматриваются процесс генерации констант алгоритмов для выбранной конфигурации. Доказывается их постоянность для одной выбранной конфигурации. Также вводится и поясняется понятие состояния, его переходы из вектора в массив и обратно.

Во второй главе проводится анализ существующих реализаций. В качестве основных параметров анализа были выбраны: область применения, предлагаемые новшества, архитектура вычислительного ядра, преимущества и недостатки реализаций. Также были оценены такие параметры, как тактовая частота устройства и затраты аппаратных ресурсов ПЛИС.

Выбор устройств осуществлялся по принципу необходимости: хеширование должно было выполнять конкретную задачу. Для этого были выбраны реализации, использующиеся в сети датчиков, сети интернет для проверки входящего трафика и т.д. Среди рассматриваемых архитектур большинство использовало последовательные схемы без использования RAM для хранения состояния.

Отобранные 5 реализаций преследовали разные цели. Были выбраны и те, для которых важна производительность, а были и те, для которых аппаратные затраты имели первоочередное значение.

В главе 3 представлена разработка устройств и их анализ. Для его создания были проанализированы различные архитектурные решения, позволяющие добиться одной из целей: увеличение производительности или уменьшение затрат ресурсов.

Особое внимание было уделено блоку перемешивания Keccak, который является основным вычислительным блоком устройства.

Большое внимание было уделено реализации устройства, способного принимать сообщения произвольной длины. Для этого необходимо было разработать интерфейс приёма-передачи, а также продумать возможное взаимодействие между вычислительными и управляющими блоками.

Разработка устройств включала следующие этапы :

– Выбор различных архитектурных решений и его аргументация;

– Разработка структур и схем блоков приёма, управления и перемешивания;

– Тестирование отдельных блоков и устройства в целом.

– Оценка основных параметров и сравнительный анализ с существующими реализациями.

Структура устройства была выбрана с учётом управления всем этапами приёма, генерации и выдачи хеш-значения. Структурная схема включает в себя четыре базовых блока: блок управления, блок приёма, блок сопряжения и блок вычисления Keccak.

Структурная схема полученного устройства представлена на рисунке 1.

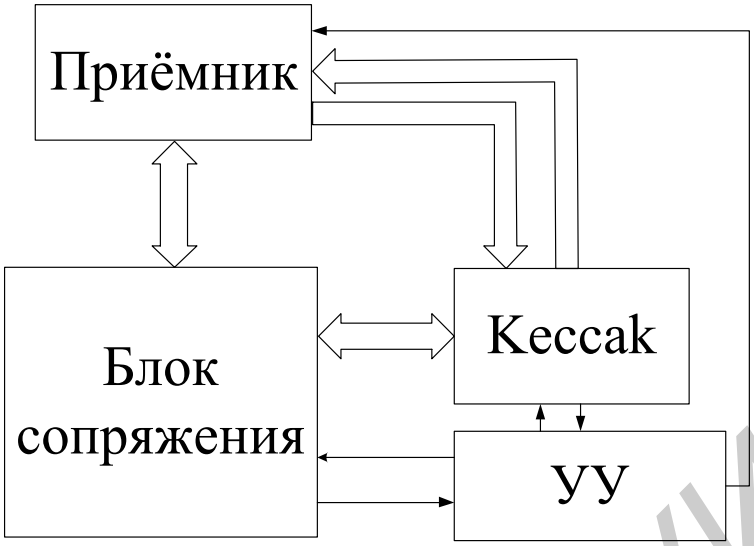

Рисунок 1 – Структурная схема полученного устройства

Приём входного сообщения осуществляется пакетами по 1088 бит каждый. Разрядность шины приёма данных равна 64 бита.

Для проектирования блока Keccak были выбраны две архитектуры, позволяющие вычислить хеш-значение: структура вычислителя с использованием архитектуры, аналогичной процессору общего назначения и структура, использующая последовательное вычисление функций.

Структурные схемы устройств представлены на рисунках 2 и 3.

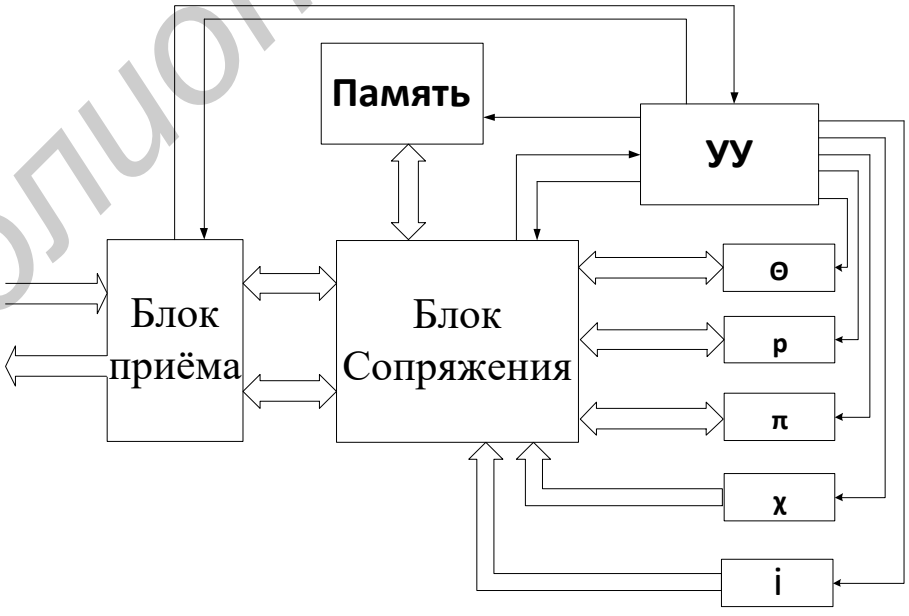

Рисунок 2 – Структура вычислителя Keccak с использованием архитектуры, аналогичной процессору общего назначения

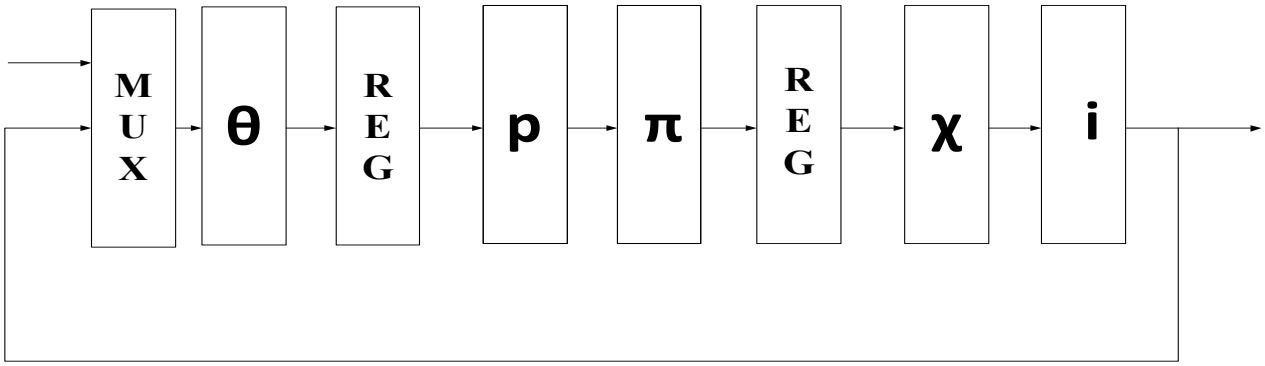

Рисунок 3 – Структурная схема вычислителя одной итерации алгоритма SHA-3, использующего последовательное вычисление функций

На основе двух структурных схем были разработаны 4 устройства. Для схемы на рисунке 2 блоки раундовых функций сначала были разделены в отдельные вычислительные блоки, а затем объединены в один общий вычислительный блок итерации. Для схемы на рисунке 3 были разработаны реализации с использованием двух и трёх регистров для уменьшения критического пути и соответственно увеличения производительности.

Тестирование устройства проводилось по уровням, начиная с блоков раундовых функций. Тестовые примеры для блоков раундовых функций, блока Keccak и всего устройства хеширования были взяты из соответствующих стандартов.

Также для проверки работоспособности итерации блока Keccak и всех промежуточных вычислений была разработана программа на языке программирования Python, с результатами которой и сверялись результаты работы блока.

Полная временная диаграмма вычислителя с использованием архитектуры, аналогичной процессору общего назначения представлена на рисунках4,5. Временные диаграммы для последовательных схем представлены на рисунках 6,7.

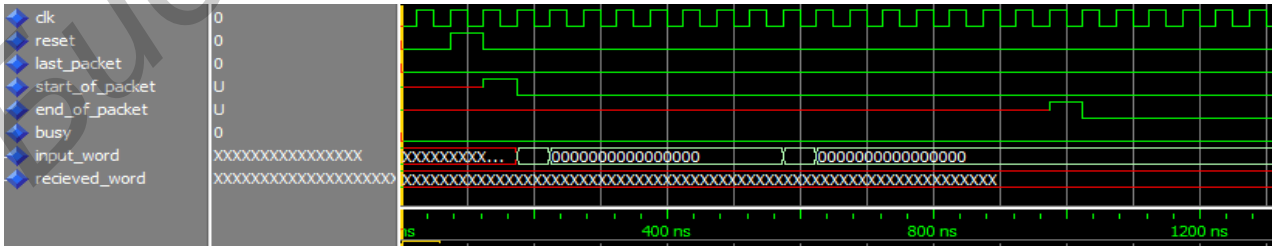

Рисунок 4– Временная диаграмма начала генерации хеш-значения

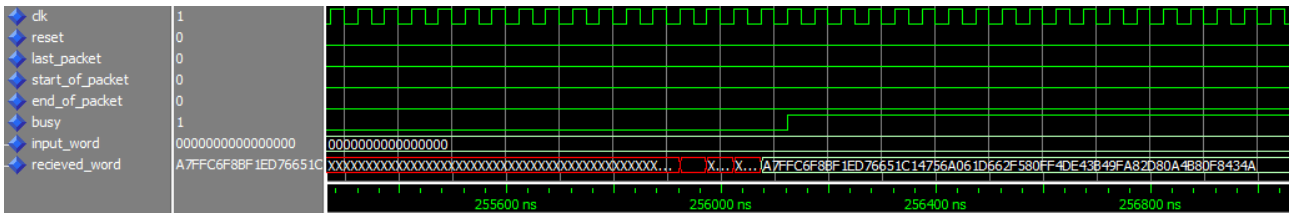

Рисунок 5 – Временная диаграмма окончания генерации хеш-значения

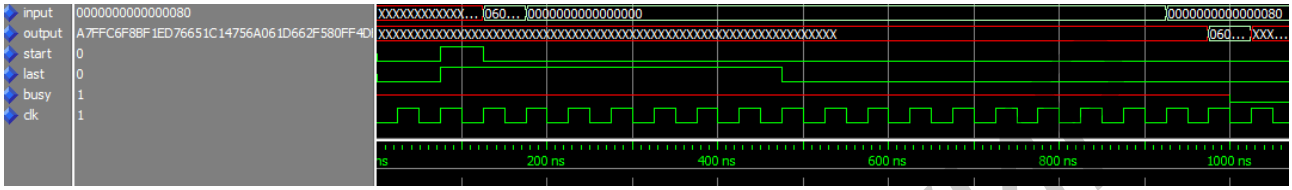

Рисунок 6– Временная диаграмма начала генерации хеш-значения для схемы с двумя промежуточными регистрами

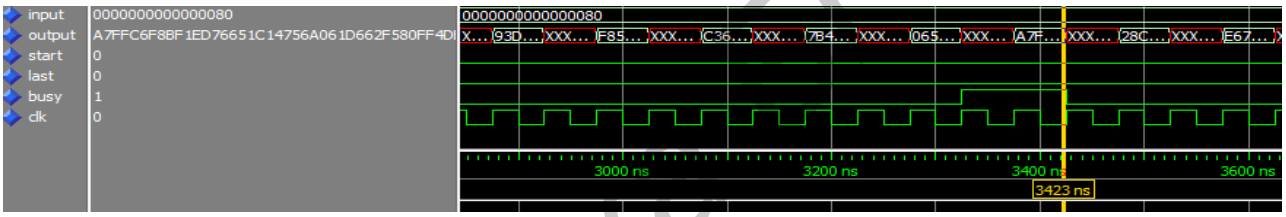

Рисунок 7– Временная диаграмма окончания генерации хеш-значения для схемы с двумя промежуточными регистрами

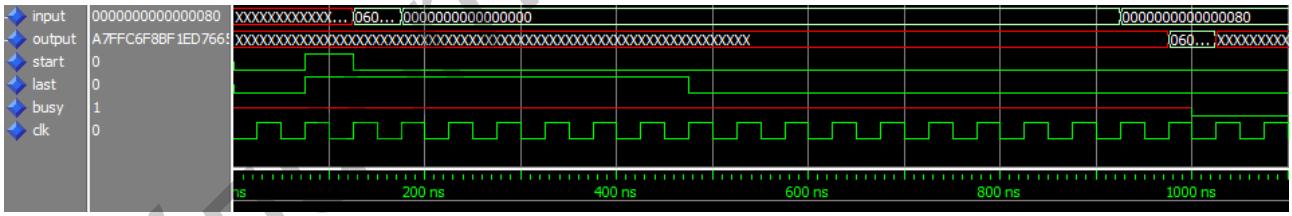

Рисунок 8 – Временная диаграмма начала генерации хеш-значения для схемы с тремя промежуточными регистрами

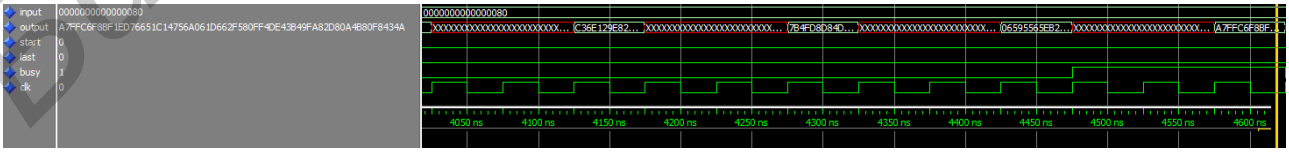

Рисунок 9– Временная диаграмма окончания генерации хеш-значения для схемы с тремя промежуточными регистрами

После проверки работоспособности устройства была проведена оценка производительности полученных устройств и их сравнение с выбранными реа-

лизациями. В таблице 1 представлены частотные характеристики полученных устройств.

Таблица 1 – Характеристики полученных устройств

Номер устройства	Архитектура	Частота МГц	Аппаратные затраты			
			slice	LUT	BRAM	FF
1	Предлагаемый процессор, блоки как отдельные узлы	128	5709	5419	1	4457
2	Предлагаемый процессор, итерация общий блок	190	3603	3478	1	1618
3	Предлагаемая последовательная схема, два промежуточных регистра	235	6009	5438	0	3345
4	Предлагаемая последовательная схема, три промежуточных регистра	240	6928	4894	0	4470
5	Последовательная схема, сеть датчиков	273	1163	-	1	-
6	Процессор, Keccak одним блоком	194,78	1048	-	1	-
7	Последовательная схема, два блока раундовых функций	287	1967	-	0	-
8	Самое экономное решение	197,85	49	193	-	-

Для кристалла ПЛИС xc7vx485t-2ffg1761 семейства Xilinx Virtex 7 полученная после процедуры синтеза максимальная тактовая частота составляет 240МГц. Полученные результаты свидетельствуют о выполнении цели и задач исследования, так как устройство быстрее практически всех рассмотренных ранее устройств.

Описание было размещено на кристалле ПЛИС. Проведена оценка затрат аппаратных ресурсов. Полученные результаты говорят о том, что использование последовательной схемы позволяет получить ощутимый прирост производительности для процессора хеширования SHA-3.

ЗАКЛЮЧЕНИЕ

Результатом проведенного исследования стала разработка полноценного устройства хеширования на основе стандарта FIPS 202. В ходе работы были рассмотрены алгоритмы, входящие в состав алгоритма хеширования SHA-3, а также семейство алгоритмов SHA-2.

В работе были проанализированы аппаратные реализации алгоритма хеширования SHA-3. Проведен анализ алгоритма стандарта FIPS 202 с точки зрения особенностей его реализации на базе ПЛИС с целью минимизации аппаратных затрат и максимизации производительности. На основе проведенного анализа были разработаны две архитектуры специализированного процессора с использованием последовательной схемы и архитектуры с выделением вычислительной части и памяти в отдельные блоки. Для полученных реализаций был проведён сравнительный анализ.

Архитектура устройств описана с помощью языка VHDL и синтезирована средствами САПР ISE 14.7. Для подтверждения работоспособности было проведено тестирование полученного устройства на тестовых примерах из стандарта FIPS, а также среди открытых наборов данных для тестирования.

Для кристалла ПЛИС xc7vx485t-2ffg1761семейства Xilinx Virtex 7 максимальная полученная после процедуры синтеза тактовая частота составляет 240МГц. Полученные результаты свидетельствуют о выполнении цели и задач исследования.

Разработанный процессор может быть встроен в любую систему, требующую проверку подлинности и целостности данных.

Дальнейшие улучшения устройства могут быть направлены на организацию схемы параллельных вычислений блоков, так как это наиболее узкое место всех реализаций с использованием последовательных схем. Также необходимо изучить возможность встраивания конвейера для организации параллельных вычислений.

Результаты диссертации были представлены на 57-й и 58-й научных конференциях аспирантов, магистрантов и студентов БГУИР.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А.] Ероховец В.А. Анализ архитектурных решений процессора SHA-3. // В.А.Ероховец. // 58-я научная конференция аспирантов, магистрантов и студентов БГУИР.

[2-А.] Ероховец В.А. Процессор SHA-3 на базе FPGA. // В.А.Ероховец. // 57-я научная конференция аспирантов, магистрантов и студентов БГУИР.