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

УДК 004.272

Корбут
Анна Александровна

Высокопроизводительная реализация HMAC SHA-256 на базе FPGA

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-40 80 01 «Элементы и устройства вычислительной техники и систем управления»

Научный руководитель
Станкевич А.В.
канд. техн. наук

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

Необходимость обеспечения конфиденциальности и сохранения целостности данных в рамках систематизации повседневной жизни бесспорна и очевидна. С увеличением потребности передачи государственных, военных, коммерческих, частных данных посредствам компьютерных сетей произошла глобализация использования защиты доступа от посторонних лиц.

Одним из методов криптографии является хеширование, – преобразование входного сообщения произвольной длины различными алгоритмами в хеш-значение фиксированной длины для достижения невозможности их расшифровки и уникальности набора символов.

Алгоритм криптографического хеширования SHA-256 разработан Агенством национальной безопасности США и опубликован в 2002 году. Является частью второго семейства алгоритмов хеширования. SHA-256 участвует в процессе аутентификации пакетов программного обеспечения Debian и в стандарте подписывания сообщений DKIM, предложен для использования в DNSSEC. Биткоин использует алгоритм для проверки транзакций, доказательства выполнения работы и доказательства доли владения. Семейство алгоритмов SHA-2 обязательно для использования в определенных приложениях правительства США, включая использование в других криптографических алгоритмах и протоколах для защиты конфиденциальной неклассифицированной информации.

Алгоритм HMAC используется для проверки целостности инфомации, с его помощью можно гарантировать невмешательство постороннего в передаваемые или хранящиеся данные. Применяется в протоколах защиты сетевого трафика, таких как IPSec, IPv6, SSL/TLS и др.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Целью диссертации является анализ возможных архитектурных решений процессора алгоритма HMAC-SHA256, позволяющих получить высокую производительность, выбор архитектуры для последующей реализации на базе FPGA и практическая реализация данного алгоритма. Указанная цель определяет следующие задачи:

1. Провести обзор известных аппаратных реализаций алгоритмов SHA256 и HMAC;
2. Выбрать архитектуру и реализовать на базе FPGA процессор алгоритма HMAC-SHA256;
3. Исследовать характеристики (аппаратные затраты и производительность) полученного процессора и провести их сравнение с известными реализациями.

Научная новизна работы заключается в архитектурных решениях процессора и его отдельных узлов, а также в исследовании их характеристик. Практическая значимость работы состоит в разработке процессорного ядра алгоритма HMAC-SHA256, которое может быть встроено в любую цифровую систему, нуждающуюся в проверке подлинности сообщений.

Диссертационная работа состоит из введения, четырех глав, заключения и двух приложений.

В первой главе освещены описание алгоритмов, принцип их функционирования. Во второй главе рассматриваюься известные аппаратные реализации алгоритмов, а также принципы организации архитектур, вошедшие в основу исследовательской работы. Третья глава описывает выбранные стратегии реализации, схемотехническое моделирование архитектуры проекта, а также отражает исходное VHLD-описание частей IP-ядра. В четвертой главе содержатся результаты проведенных тестов и сравнительный анализ с ранее рассмотренными реализациями, а также программа верификации.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Задачей данного проекта является разработка быстродействующей архитектуры специализированного процессора, предназначенного для выполнения алгоритма HMAC-SHA256, и его реализация на базе FPGA. Высокая производительность будет достигаться путем параллельно-итеративно-конвейерной реализации двух алгоритмов. Вся схема реализуется аппаратно, без использования предварительной программной обработки входящих ключа и сообщения. Общую схему стоит рассматривать как составную из нескольких основных функциональных блоков, каждый из которых, в свою очередь, разделяется на собственные подблоки.

Обобщенная структурная схема изображена на рисунке 1.

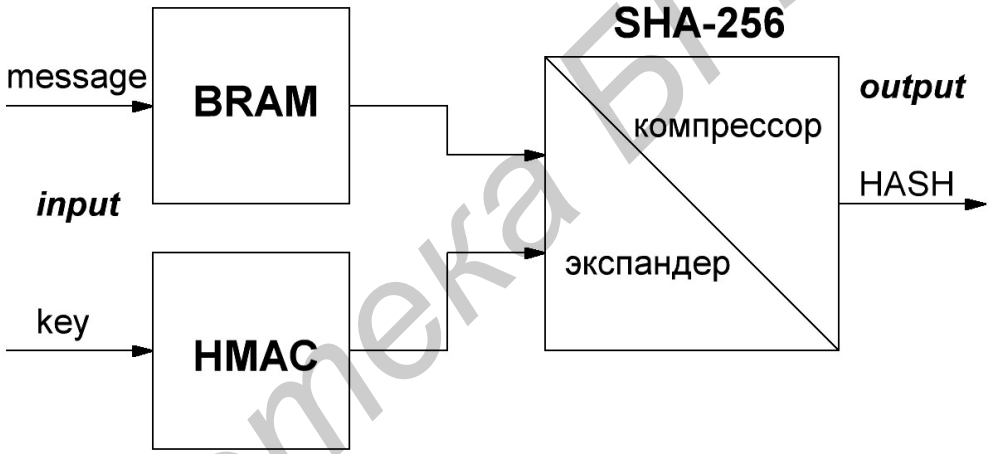

Рисунок 1. – Укрупненная структурная схема

На рисунке 2 показана разработанная структурная схема проекта. Процессор начинает свою работу по активному уровню входного сигнала *"start"*. Сообщение поступает через входную 32-битную шину "input" и накапливается в блочной памяти BRAM. Окончание приема сообщения определяется входным сигналом *"in_stop"* и сигналом *"n_bit"*. Сигнал *"n_bit"* устанавливает количество значащих бит в последнем принятой части сообщения (*"input"*).

Ключ, необходимый для расчета алгоритма HMAC, поступает через входную 32-битную шину *"key"*. Входные сигналы *"key_stop"* и *"key_bit"* обозначают окончание приема ключа и количество значащих бит в последней принятой части ключа *"key"* соответственно. Был определен максимально допустимый размер ключа с условием его достаточной защищенности, равный размеру блока алгоритма SHA-256(512 бит), для

упрощения вычислений алгоритма HMAC и уменьшения затрат ресурсов ПЛИС.

Входные части ключа и сообщения проходят этап предобработки в блоках *KEY_PREPROC* и *MESSAGE_PREPROC*.

Сообщение дополняется единицей и вычисляется его размер в битах (без учета дополнения). Затем сообщение дополняется до нужной длины путем формирования 32-битных слов, заполненных нулевыми битами. Последнее слово содержит размер сообщения. Полученные слова поочередно записываются в блочную память для последовательного извлечения.

Под предобработкой ключа понимается вычисление его размера и дополнение до 512-го бита, в случае меньшего размера, нулевыми битами. Сформированные 32-битные слова последовательно подаются в дальнейшую обработку.

Первые 64 такта входной ключ преобразовывается путем операции "сложение по модулю 2" с соответствующими константами (ipad и opad) и подается в обработку двух блоков *SHA-256*. Обработка блоком SHA-256 происходит за 70 тактов. Результаты первой обработки блока SHA-256 key сохраняются для использования в финальном вычислении. Выходные значения блока *SHA-256 message* через мультиплексор перезагружаются в блок в качестве входа до тех пор, пока дополненное входное сообщение не будет обработано.

С 70-ого такта формируется адрес чтения сообщения из блочной памяти, и сообщение поступает на вход блока *SHA-256 message* в качестве входного сигнала *"word"*.

После вычисления дайджеста значения, полученного склеиванием блока ключа с входным сообщением, начинается второй этап обработки. В одном из блоков дайджест преобразуется в 32-битные слова 512-битного блока нового сообщения. Сохраненные значения с блока *SHA-256 key* поступают на вход блока *SHA-256 message* в качестве стартовых значений переменных *A-H* и рассчитывается финальное hash-значение.

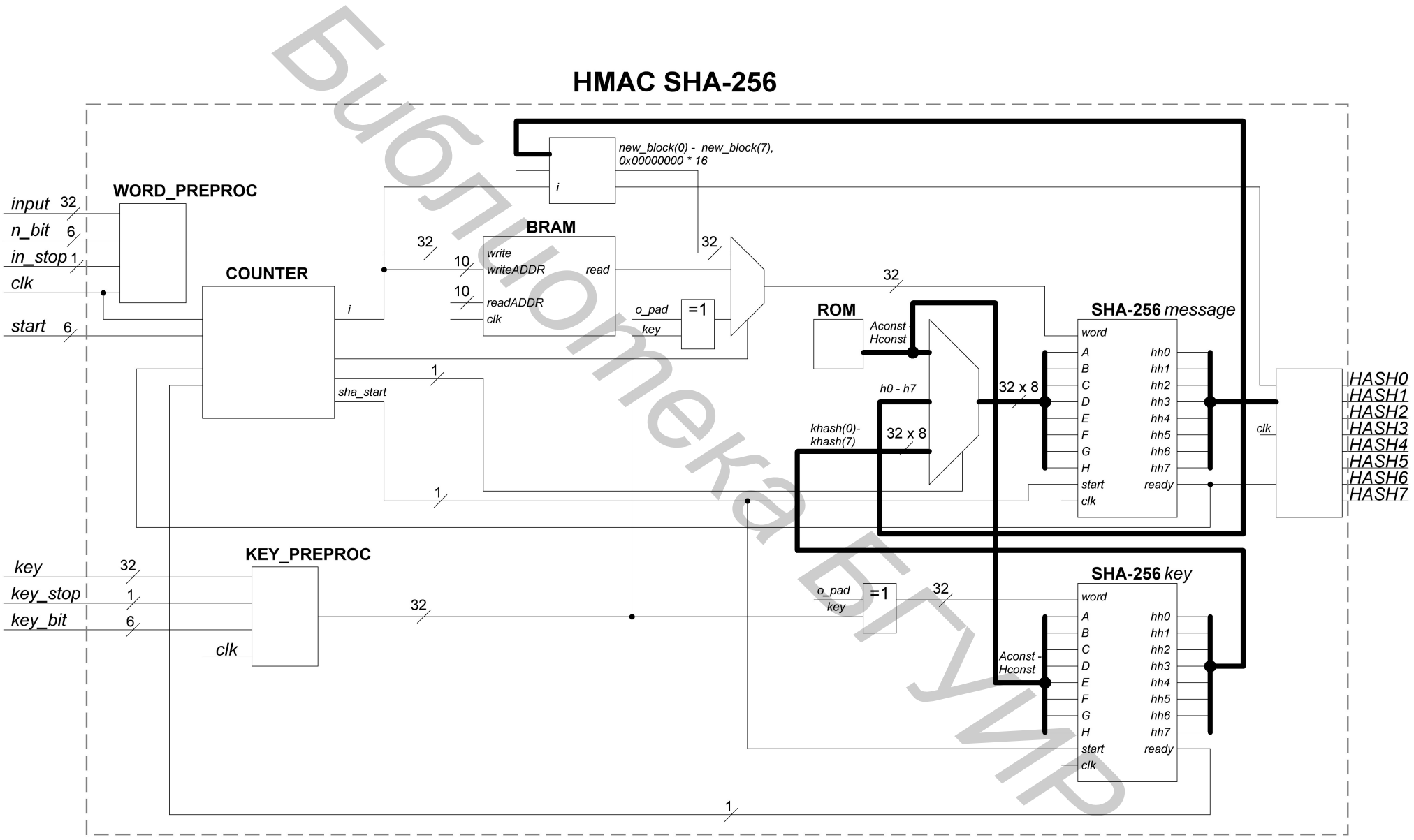

Рисунок 2. – Схема HMAC SHA-256

Для внутренних блоков алгоритма SHA-256, экспандера и компрессора, разработаны быстродействующие схемы

Компрессором называется блок, выполняющий вычисления главного цикла. В классических реализациях одна итерация 64-ступенчатого цикла выполняется за один такт. Для быстродействия данный принцип упразднен. Операции, которые должны быть вычислены за одну итерацию цикла, распределяются на три такта, для уменьшения критического пути одного такта. Также для ускорения сложения используется разработанный сумматор с тремя входами. Разработанная схема компрессора изображена на рисунке 3.

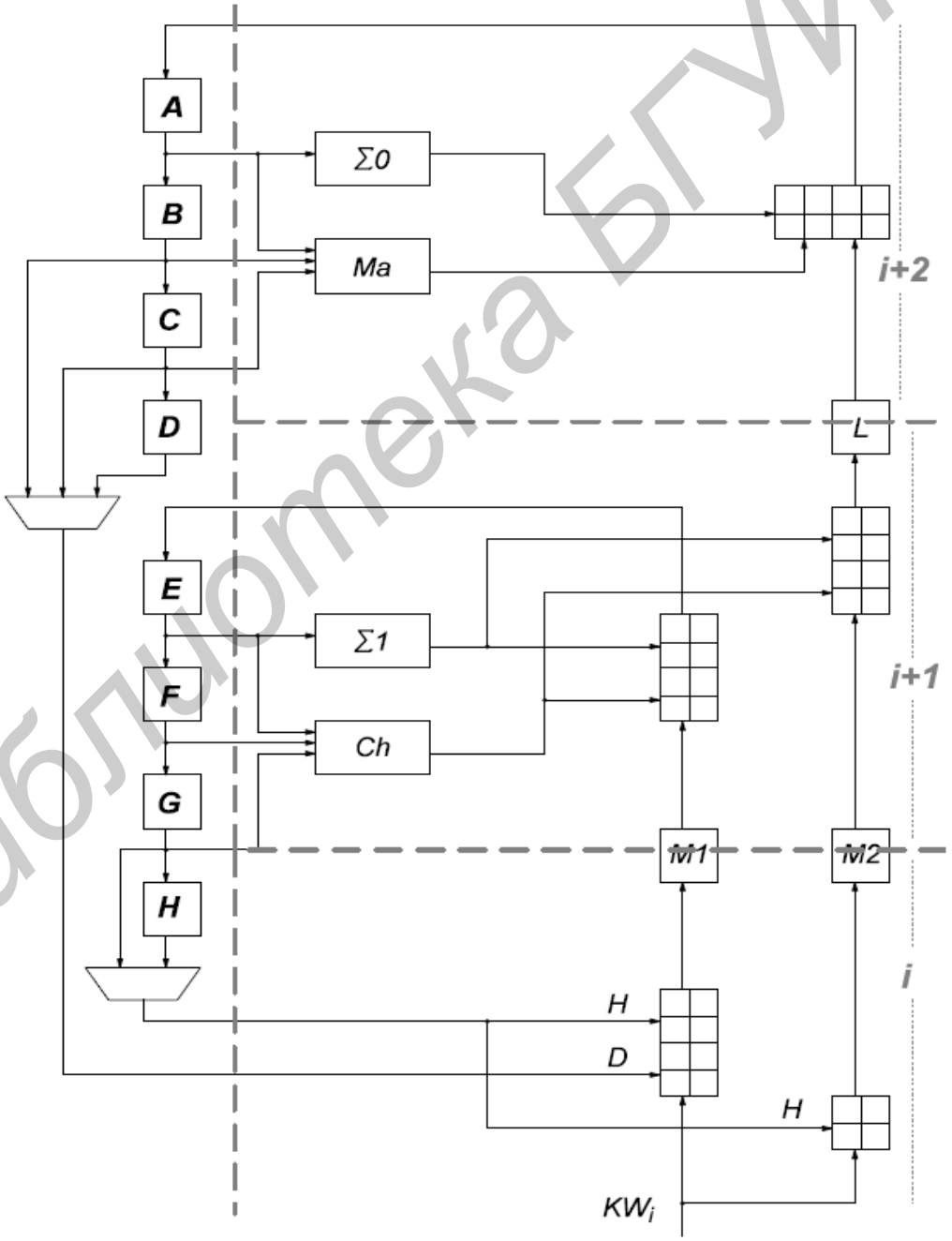

Рисунок 3. – Схема компрессора

Критическим путем для данной реализации является вычисление двух простейших логических функций и сложение полученных результатов со значением одного из регистров.

В классической реализаци экспандер рассчитывает слова W, получаемые из очередного 512-битного блока входного сообщения(пункт 1.1.3). Для наиболее быстрого расчета этап сложения очередного значения W с константой K был перенесен в рассматриваемый блок. Экспандер разрабатывался с задачей получить задержку такта сопоставимую с задержкой такта в компрессоре, но не больше ее. Реализованная схема показана на рисунке 4. Она состоит из шестнадцати сдвиговых регистров, трех сумматоров с тремя входами и мультиплексора. Так же, как и части компрессора схема отрабатывает за два последовательных такта. Именно поэтому она условно разделена на две части в соответствии с выполнением каждой в тактах t, $t+1$.

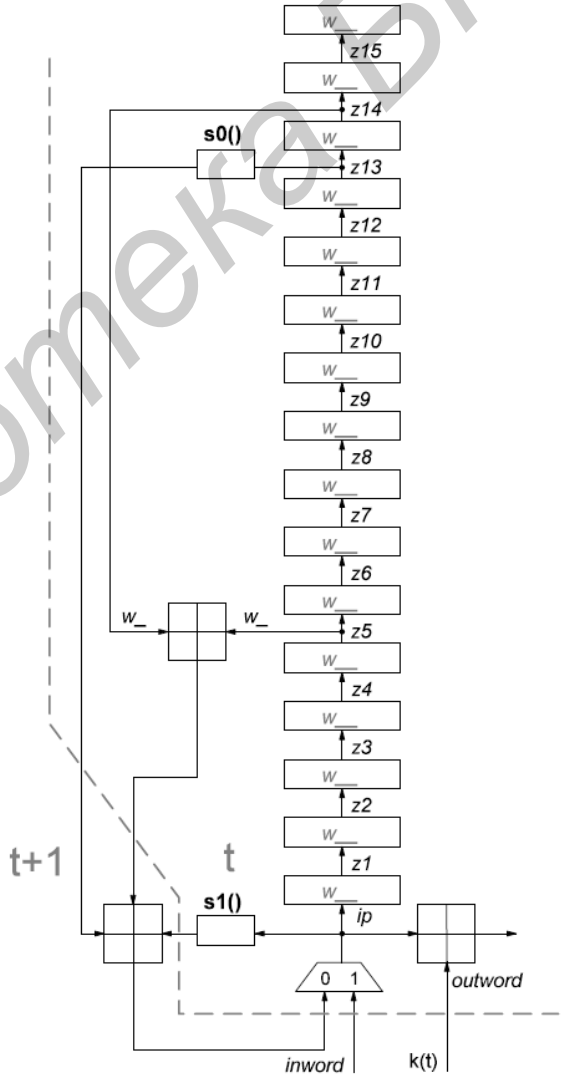

Рисунок 4. – Структурная схема экспандера

Для реализации проекта использовалась среда разработки программируемых логических интегральных схем Xilinx Vivado версии v2019.1. В ходе реализации схем было написано несколько проверочных программ для проведения тестов реализации. Для написания использовался язык программирования Си.

Для проведения синтеза выбрано устройство Xilinx семейства Virtex - 7, xc7vx330tffg1157-3, результат используемых ресурсов ПЛИС приведен на рисунке 5.

Resource	Estimation	Available	Utilization %
LUT	2717	362800	0.75
LUTRAM	128	141600	0.09
FF	3396	725600	0.47
BRAM	1	940	0.11
IO	336	400	84.00
BUFG	1	80	1.25

Рисунок 5. – Результаты синтеза проекта Virtex7

Для рассмотрения результата полученных временных задержек из отчета вынен рисунок 6.

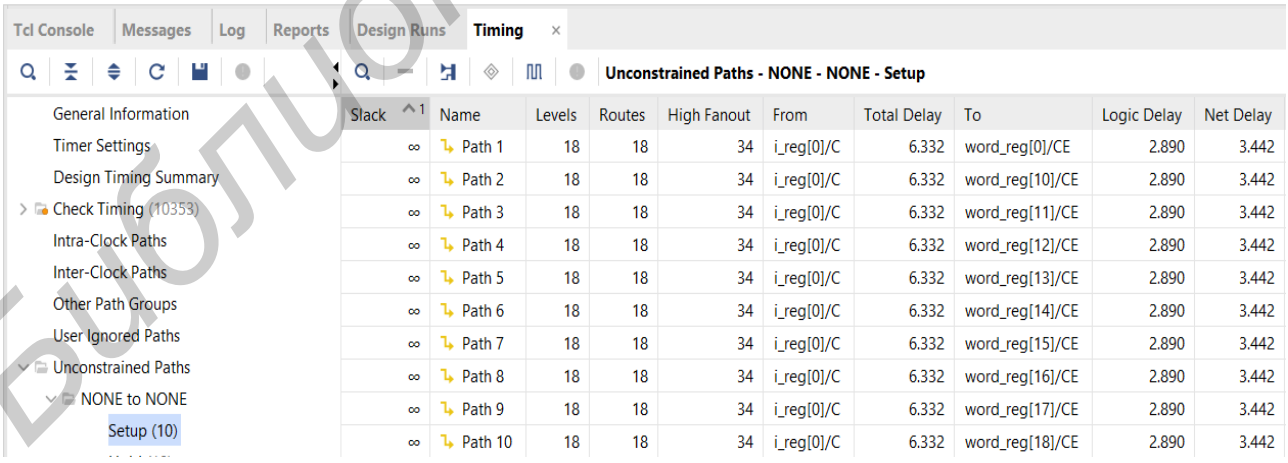

Рисунок 6. – Временные показатели Virtex7

По формуле (1) получена частота:

$$\upsilon = \frac{1}{T} = \frac{1}{6,332 * 10^{-9}} = 158 \text{ МГц} \quad (1)$$

ЗАКЛЮЧЕНИЕ

В диссертационной работе был проведен анализ возможных архитектурных решений специализированного процессора алгоритма HMAC-SHA256, позволяющих получить высокую производительность.

На основе проведенного анализа выбрана смешанная итеративно-конвейерная архитектура SHA256 с использованием распараллеливания вычислений на уровне приема сообщения и вычисления HMAC.

Указанная архитектура описана на языке VHDL и синтезирована средствами САПР Vivado 2019. Для подтверждения работоспособности разработанного устройства написана программа для получения значений в требуемых точках алгоритма вычислений, а также проведено тестирование процессора на известных сообщениях. Тестирование подтвердило правильность функционирования устройства.

Исследованы характеристики (аппаратные затраты и производительность) разработанного процессора при его реализации на FPGA 7 серии Xilinx. Предлагаемая реализация по сравнению с известными имеет примерно сопоставимую производительность, однако требует на 20-30% меньше аппаратных ресурсов кристалла ПЛИС.

Результаты разработки свидетельствуют о выполнении цели и всех задач исследования.

Разработанный процессор алгоритма HMAC-SHA256 может быть использован как IP-ядро в системах, требующих высокопроизводительной проверки подлинности сообщений.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1-А] Корбут А.А. Высокопроизводительная реализация алгоритма HMAC SHA-256 на базе FPGA / А.А. Корбут // Компьютерные системы и сети: 56-я научная конференция аспирантов, магистрантов и студентов, Минск, 21-24 апреля 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2020. – С. 223 – 224. (https://www.bsuir.by/m/12_100229_1_144999.pdf)