АНАЛИЗ АРХИТЕКТУРНЫХ РЕШЕНИЙ ПРОЦЕССОРА SHA-3

Ероховец В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станкевич А.В. – канд. техн. наук)

Развитие информационных технологий требует постоянного совершенствования средств, обеспечивающих информационную безопасность. Криптографические хэш-функции используются в алгоритмах цифровой подписи, для проверки подлинности и целостности полученного сообщения и позволяют вычислить для произвольного сообщения переменой длины хэш-значение фиксированной длины. Одна из таких функций описывается алгоритмом SHA-3, принятым в 2015 году в качестве стандарта Национальным институтом стандартов и технологий США (NIST).

SHA-3 (Keccak) – алгоритм хеширования сообщений переменной длины. В алгоритме предложено использовать новое решение, такое как криптографическая губка. При таком решении процесс вычисления хэш-значения разбивается на два этапа: впитывание – преобразование блоков входного сообщения с помощью функции перемешивания; и отжимание – выделение из вектора состояний частей итогового хеш-значения и дальнейшее преобразование с помощью функции перемешивания. Структура конструкции губки представлена на рисунке 1 [1].

Алгоритм перемешивания представляет собой итеративный алгоритм с заранее заданным числом итераций, что позволяет использовать как схемы с обратной связью (итеративные вычислительные устройства), так и реализовывать конвейерные вычисления. Используемые внутри него раундовые функции модифицируют введённый в стандарте массив состояний, который формируется из входного вектора сообщения. Следует иметь в виду, что поскольку длина входного сообщения заранее не известна, то количество использований функции перестановки f (рисунок 1) будет переменной величиной. В зависимости от требуемых характеристик устройства, возможны несколько вариаций архитектур [2].

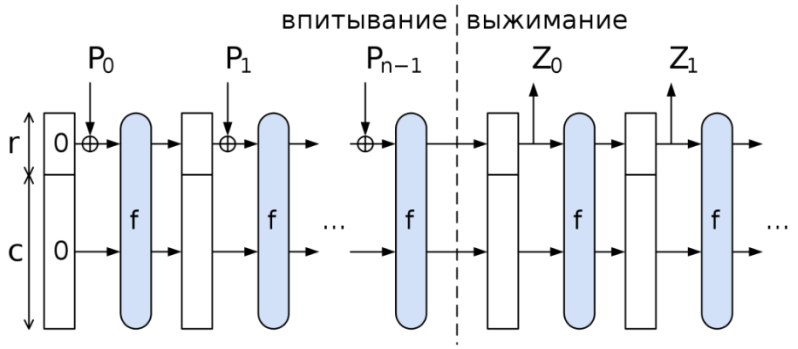

Рисунок 1 – Структурная схема блока, выполняющего функцию “криптографической губки”

Для сравнения были выбраны архитектура с использованием блока управления и памяти, представленная на рисунке 2, и вычислительного блока, использующего последовательное вычисление шагов раунда алгоритма, представленная на рисунке 3.

Основными различиями архитектур стал подход к организации вычислений и хранению массива состояния. Для архитектуры с блоком управления и памятью необходимо иметь некоторое количество состояний, которые описывают процесс вычисления в конкретный момент. Этими состояниями и оперирует блок управления. Вычисление раундовых функций выделено в отдельные вычислительные блоки, которые взаимодействуют с памятью массива состояний через устройство управления [3].

Использование последовательной схемы обусловлено отказом от хранения массива состояний в памяти. Вследствие этого схема вычислений приобретает несколько другой вид. При организации вычислений раундовых функций друг за другом в одной схеме необходимо передавать изменённый в предыдущем блоке массив на блок следующей раундовой функции. Для организации цикла в схеме используется мультиплексор, который позволяет подать на вход вычислителя стартовый вектор или выходной вектор предыдущего такта работы алгоритма для корректной работы устройства [3].

В обоих рассмотренных случаях необходимо внешнее управление процессом вычисления и приёма входного сообщения. В схеме вычисления SHA-3 данные процессы выделены в отдельные структурные блоки. Полная структурная схема устройства, реализующего стандарт хеширования SHA-3, представлена на рисунке 4.

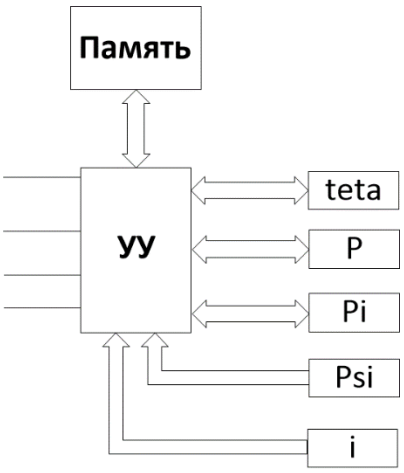

Рисунок 2 – Структурная схема вычислителя Keccak на основе архитектуры процессора общего назначения

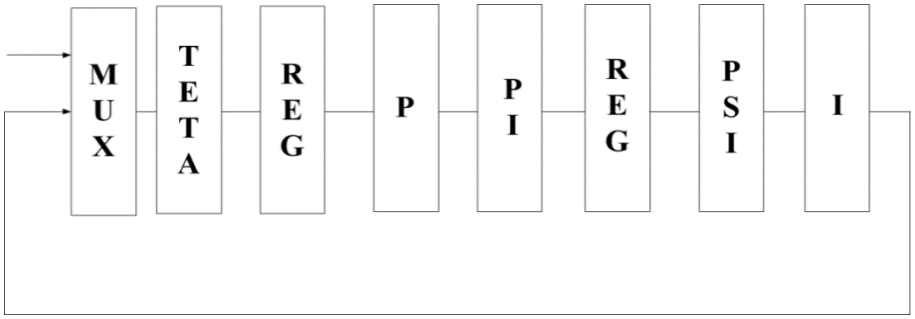

Рисунок 3 – Структурная схема вычислителя Keccak, использующего последовательное вычисление шагов раунда алгоритма

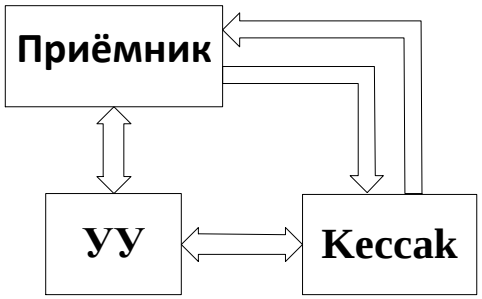

Рисунок 4 – Структурная схема предлагаемого устройства

Полученные архитектурные решения описаны на языке VHDL и реализованы в среде Xilinx ISE. Их сравнение проводилось по следующим критериям: пропускная способность, производительность, выраженная в тактовой частоте устройства и занимаемых ресурсах кристалла FPGA. Сравнительная характеристика реализаций для кристалла XC6SLX75T представлена в таблице 1.

Таблица 1 – Результаты операции place-and-route аппаратных реализаций устройств

Реализация	Тактовая частота(МГц)	Slice	LUT
С памятью	130	824	2418
Последовательная	210	1311	5235

Полученные результаты позволили сделать вывод о целесообразности использования той или иной архитектуры устройства хеширования на основе алгоритма SHA-3. Были оценены основные параметры устройства, критически важные для конечных пользователей.

Список использованных источников:
1. Wikipedia[Электронный ресурс]. – Электронные данные. – Режим доступа: https://ru.wikipedia.org/wiki/SHA-3/
2. OpenCores[Электронный ресурс]. – Электронные данные. – Режим доступа: https://opencores.org/projects/sha3
3. Compact FPGA Implementations of the Five SHA-3 Finalists. / S. Kerckhof [et al.]// Researchgate, January 2011. P.71-74