ПРОЦЕССОР SHA-3 НА БАЗЕ FPGA

Ероховец В.А.

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

Станкевич А.В. – канд. техн. наук)

Современные цифровые системы используют алгоритмы хеширования для обеспечения конфиденциальности личных данных своих пользователей. Вместе с тем, бурный рост производительности вычислительной техники ставит под сомнение безопасность алгоритмов, разработанных 10-15 лет назад. В качестве примера можно рассмотреть криптоалгоритм SHA-2, который широко использовался ранее, а сейчас заменён на современный, более надежный алгоритм SHA-3.

Алгоритм хеширования SHA-3 представляет собой новую концепцию формирования хеш-значения сообщения. SHA-3 – алгоритм хеширования переменной разрядности. В качестве официального криптоалгоритма для SHA-3 был выбран алгоритм Keccak. Он разработан в 2012 году группой авторов во главе с Йоаном Дайменом. 5 августа 2015 года алгоритм был принят в качестве стандарта FIPS 202. [1]

Алгоритм SHA-3 состоит из нескольких этапов: дополнения сообщения и функции “губки”. Так как блоки, которыми оперирует алгоритм, кратны некоторому числу r, в алгоритм включено дополнение сообщения. Однако, алгоритм, выполняющий дополнение, отличается от алгоритма дополнения SHA-2: к сообщению добавляется единичный бит, после него определенное количество (от 0 до r-1) нулевых битов, и в конце еще один единичный бит. r-1 нулевых битов может быть добавлено в случае, когда последний блок сообщения имеет длину r-1 бит. Тогда этот блок дополняется единичным битом, а следующий блок будет состоять из r-1 нулей и единицы. [1]

Основным блоком в структуре алгоритма является функция “губки”. Дополненное входное сообщение разбивается на блоки, которые затем последовательно складываются по модулю 2 со строкой состояния. Массив строк состояний формируется на каждом этапе работы алгоритма. После n итераций “впитывания”, выполняется обратный процесс “отжимания”, в ходе которого части промежуточных результатов извлекаются и составляют итоговое значение. Структура блока представлена на рисунке 1.

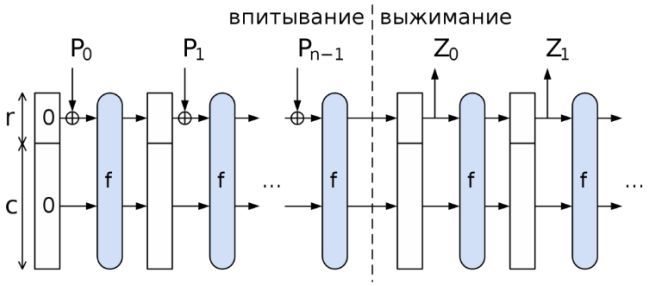

Рисунок 1 – Структурная схема блока, выполняющего функцию “губки”

При аппаратной реализации необходимо учитывать несколько факторов. Среди них произвольная длина сообщения и большой размер массива состояний S. Алгоритм не содержит блоков умножения и деления, что позволяет эффективно реализовывать алгоритм на FPGA. Этот фактор и стал определяющим в выборе данного алгоритма в качестве национального стандарта.

Алгоритм имеет множество реализаций на языках описания аппаратуры. В таблице 1 приведены результаты операции place-and-route на кристаллах семейства Virtex-6.

Таблица 1 – Результаты операции place-and-route некоторых аппаратных реализаций.

Реализация	Тактовая частота (МГц)	Slice	LUT
[2]	188,9	2 220	9 895
[3]	250	144	610
[4]	291,21	1 015	-
[5]	754,32	1 171	4 635

Тактовая частота одной из реализаций процессора SHA-2 составляет 218,9 МГц [6] и практически идентична тактовой частоте процессора SHA-3. Приведенные данные позволяют сделать вывод, что алгоритм хеширования SHA-3 при аппаратной реализации имеет производительность, сопоставимую с производительностью реализаций SHA-2, обеспечивая при этом более высокую криптостойкость.

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
4. Novel Arithmetic Architecture for High Performance Implementation of SHA-3 Finalist Keccak on FPGA Platforms. / Kashif Latif [et al.] // Proceedings of the 8th international conference on Reconfigurable Computing: architectures, tools and applications, 2012. – P 496- 502.
5. Beyond the Limits: SHA-3 in just 49 Slice./ V. Arriba // 29th International Conference on Field Programmable Logic and Applications (FPL), 2019. – P.130-135
6. Design of high-throughput SHA-256 hash function based on FPGA. / S. Suhaili // 6th International Conference on Electrical Engineering and Informatics (ICEEI), 2017. – P.247-251.