АППАРАТНАЯ РЕАЛИЗАЦИЯ МОДУЛЯ ПРЕОБРАЗОВАНИЯ ХЭШ-ФУНКЦИИ SHA-512 НА БАЗЕ FPGA

М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Криптографическая хэш-функция SHA-512 предназначена для получения хэш-значения фиксированной длины для входного сообщения произвольной длины. Данная функция используется для проверки целостности данных, а также в рамках других криптографических алгоритмов и протоколов в различных приложениях, связанных с защитой информации. Поскольку функция SHA-512 использует в своей работе 64-битные слова, она является самой сильной среди функций семейства SHA-2 с точки зрения устойчивости к коллизиям и взлому. Чтобы соответствовать ограничениям

реального времени в современных приложений, возникает необходимость высокопроизводительных аппаратных реализаций алгоритма SHA-512. Эти реализации должны быть нацелены на обеспечение требуемых показателей пропускной способности и пропускной способности/объема ресурсов с помощью соответствующих методов оптимизации. В докладе рассматривается аппаратная реализация модуля преобразования хэш-функции SHA-512 на базе FPGA.

Поскольку критический путь алгоритма SHA-512 находится в раунде преобразования, основная оптимизация относится к этому модулю. Модуль преобразования реализуется с использованием набора одновременно применяемых методов оптимизации [1]. Эти методы включают как методы алгоритмического уровня (развертывание цикла, предварительное вычисление, ресинхронизация), так и методы схемного уровня, такие как перераспределение ресурсов и использование специальных модулей сумматоров с сохранением переноса (CSA).

Основной особенностью рассматриваемой реализации заключается в применении развертывания цикла в алгоритме SHA-512 [1]. При этом, как показано в [1], наилучшее значение показателя пропускная способность/объем ресурсов достигается при коэффициенте развертывания, равном 2. В этом случае два последовательных раунда объединяются вместе, образуя один новый раунд, который реализует одну операцию за итерацию, где значения рабочих переменных a(t+1) - h(t+1)) вычисляются на основе значений a(t-1) - h(t-1). При таком объединении критический путь одной итерации алгоритма становится длиннее, однако при этом число итераций уменьшается с 80 до 40.

На следующем этапе [1] осуществляется перераспределение компонентов архитектуры и использование сумматоров с сохранением переноса CSA, что приводит к уменьшению задержки критического пути.

Характеристики реализации по отчету средств синтеза пакета Vivado 2021.2 для кристалла FPGA Virtex UltraScale+ xcu250-figd2104-2L-e: 832 триггеров секций, 1051 просмотровая таблица (LUT), тактовая частота – 500 МГц.

Список литературы

1. Athanasiou G.S., Michail H.E., Theodoridis G., Goutis C.E. Optimising the SHA-512 cryptographic hash function on FPGAs // IET Comput. Digit. Tech. 2014. Vol. 8, iss. 2. P. 70–82.