КОНВЕЙЕРНАЯ РЕАЛИЗАЦИЯ 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 и используется в рамках криптографических алгоритмов и протоколов в различных приложениях, связанных с защитой информации. В ряде таких приложениях для обеспечения реального времени требуется высокопроизводительная аппаратная реализация алгоритма SHA-512. В докладе рассматривается конвейерная реализация хэш-функции SHA-512 на базе FPGA, позволяющая повысить производительность.

При конвейерной реализации алгоритма SHA-512 на базе FPGA важным вопросом является выбор архитектуры, оптимизированной с точки зрения таких параметров аппаратной реализации, как пропускная способность и пропускная способность/ресурсы кристалла. На алгоритмическом уровне для реализации алгоритма SHA-512 предлагается использовать подход, рассмотренный в работе [1]. Основной целью этой работы была разработка универсального модуля мега-раунда, позволяющего строить множество альтернативных конвейерных архитектур, обеспечивающих различные реализации алгоритма SHA-512 в FPGA фирмы Xilinx с точки зрения частоты и используемых ресурсов ПЛИС. Такие архитектуры начинаются от итеративного варианта, использующего один модуль мега-раунда, циклически реализующего все итерации алгоритма SHA-512, до полностью конвейерной архитектуры с 40 модулями мега-раундов. Анализ оптимизированного варианта мега-раунда, предлагаемого в работе [1], показывает, что окончательный критический путь состоит из двух блоков сумматоров с сохранением переноса CSA и двух нелинейных функций. Проведенные исследования показали, что проект процессора, использующий полностью конвейерную реализацию алгоритма SHA-512, предлагаемую в работе [1], система проектирования Vivado, не может реализовать на тактовой частоте 250 МГц.

В докладе предлагается модифицированный вариант мега-раунда, позволяющий уменьшить критический путь до одного 3-входового сумматора и одной нелинейной функции. Простое размещение регистров на выходе мега-раунда не приводит к уменьшению критического пути. Для уменьшения критического пути до одного

3-входового сумматора и одной нелинейной функции необходимо перенести ряд сумматоров CSA вместе с соответствующими нелинейными функциями из этапа предвычислений в пост-вычислительный этап. Кроме того, мега-раунд для удобства реализации разбивается на два модуля соответственно для каждого из этапов. В каждом из этих модулей критический путь состоит из одного 3-входового сумматора и одной нелинейной функции. Весь конвейер реализации алгоритма SHA-512 с учетом входного буфера для вектора инициализации алгоритма формирует хэш-значение за 85 тактов.

Характеристики реализации по отчету средств синтеза пакета Vivado 2021.2 для кристалла FPGA Virtex UltraScale+ xcu250-figd2104-2L-e: 96963 триггеров секций, 82197 просмотровая таблица (LUT), тактовая частота – 250 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, pp. 70-82 [Электронный ресурс]. – Режим доступа: https://ietresearch.onlinelibrary.wiley.com/doi/epdf/10.1049/iet-cdt.2013.0010. – Дата доступа: 02.05.2024.