ИСПОЛЬЗОВАНИЕ DSP БЛОКОВ FPGA ФИРМЫ XILINX ДЛЯ РЕАЛИЗАЦИИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ М.В. Качинский, А.В. Станкевич, А.И. Шемаров

Одним из основных требований к современным системам цифровой обработки информации является высокая производительность. Достигнуть высокой скорости вычислений можно с помощью методов параллельной обработки, удобных для реализации в ПЛИС. FPGA фирмы Xilinx позволяют существенно увеличить производительность реализации алгоритмов обработки информации за счет использования параллельно работающих аппаратных узлов, размещенных на кристалле ПЛИС. Современные FPGA, кроме собственно логических ресурсов

и блоков ввода-вывода, содержат большое количество аппаратных блоков, реализующих часто используемые в цифровой схемотехнике операции. Аналогичные узлы, выполненные на просмотровых таблицах (LUT), требуют больше ресурсов кристалла и имеют пониженное быстродействие. В то же время аппаратная реализация этих блоков несущественно увеличивает площадь кристалла и стоимость ПЛИС, однако при этом заметно улучшает характеристики проекта в целом [1]. Одним из видов таких узлов являются блоки DSP (цифровой обработки сигналов). В докладе рассматривается использование DSP блоков в FPGA семейства Virtex-7 фирмы Xilinx для реализации различных конвейерных криптографических алгоритмов. Для иллюстрации используется алгоритм шифрования данных стандарта DES, который хорошо пригоден для конвейерной обработки.

FPGA семейства Virtex-7 фирмы Xilinx содержат блоки DSP48E1 [2]. В общем случае блоки DSP48E1 предназначены для реализации алгоритмов цифровой обработки сигналов и содержат избыточные для криптографических алгоритмов узлы такие, как умножитель, предварительный сумматор и некоторые другие. В криптографических алгоритмах блоки DSP48E1 могут использоваться в упрощенной конфигурации для реализации арифметических и логических операций, а также операции сравнения. Например, с помощью блоков DSP48E1 могут выполняться операции XOR для раундов алгоритма DES. В версии алгоритма DES, удобной для конвейерной реализации, эта операция 4-входовая, поэтому вычислительный модуль для раундов строится на трех блоках DSP48E1. Задержка выполнения операции XOR в блоках DSP48E1 составляет 4 такта, общая задержка модуля составляет 5 тактов синхронизации. Такой подход позволяет получить более экономичную реализацию конвейера алгоритма шифрования данных в целом за счет уменьшения количества используемых LUT кристалла FPGA.

Литература

1. Тарасов И. ПЛИС Xilinx и цифровая обработка сигналов. Особенности, преимущества, перспективы // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. – 2011. – № 3.

2. 7 Series DSP48E1 Slice User Guide: [Электронный ресурс]. – Режим доступа: https://www.xilinx.com/support/documentation/user_guides/ug479_7Series_DSP48E1.pdf. – Дата доступа: 10.05.2020.