АНАЛИЗ АППАРАТУРНЫХ ЗАТРАТ НА РЕАЛИЗАЦИЮ ЦИФРОВОГО УСТРОЙСТВА ВСЕВОЗМОЖНЫХ ПЕРЕСТАНОВОК

Кохновский С.И.

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

Иванюк А.А. – д.т.н.,профессор

Целью работы является анализ аппаратных затрат при размещении цифрового устройства всевозможных перестановок на кристалле семейства Artix 7.

В современном мире как никогда актуальна проблема защиты авторских прав. Все объекты интеллектуальной собственности могут подвергаться атакам злоумышленников в совершенно непредсказуемое время. Для обеспечения большей трудоёмкости доступа к защищенной информации применяются различные методы, в том числе запутывающие устройства, однозначно отображающие входные сигналы на выходные в зависимости от подаваемого ключа. Далее будет

рассмотрено одно из таких устройств.

На входы комбинационной схемы подаются *N* бит входных сигналов и *M* бит ключа. Стоит заметить, что $M = \frac{N}{2} * (N - 1)$. На выходы подаются *N* бит – запутанная последовательность. Пусть рассматривается устройство размерностью *N* = 2. Вычислив *M*, получим 1. Таким образом, соответствие входных и выходных сигналов одинакового порядкового номера будет прямым, если ключ был равен 0, и обратным в противном случае. Обобщение работы устройства на размерность любого *N* представлено в работе [1].

Следует рассмотреть характеристики и оценить аппаратурные затраты на реализацию цифрового устройства, которое может быть расположено на кристалле серии Artix-7 компании Xilinx. Кристаллы программируемой логики серии Artix-7 относятся к ПЛИС, эффективно используемым в настоящее время [2].

В процессе синтеза комбинационного устройства для *N* = 18 исчерпывается количество портов ввода и вывода, что обусловлено аппаратными характеристиками кристалла. На кристалле XC7A200T, который использовался для синтеза и моделирования устройства, имеется лишь 500 портов. Решением проблемы дефицита портов является механизм периферийного сканирования: последовательно передавая сигналы, которые поступают на вход, и сигналы ключа, есть возможность добиться сокращения количества используемых входов и выходов на кристалле до константы – 5, однако появляется необходимость в использовании сигналов синхронизации *clk* и разрешения *en*. После внедрения вышеописанных измерений комбинационная схема становится последовательной цифровой схемой с некоторой комбинационной частью (рисунок 1). Очевидно, что при увеличении размерности комбинационной части, ни логика, ни аппаратные затраты на реализацию последовательной части не возрастают, будет изменяться лишь количество тактов между повторной установкой сигнала *en*.

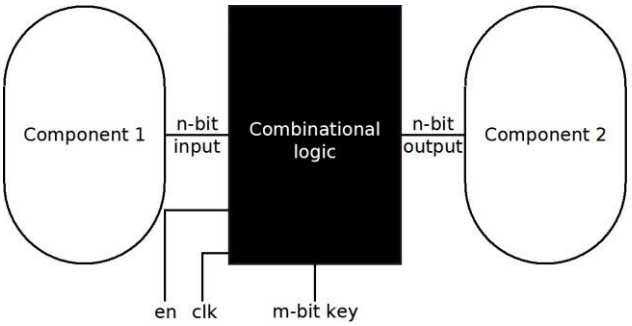

Рисунок 1. Схема последовательного цифрового устройства

Аппаратные ресурсы ПЛИС ограничены количеством срезов (slices), которые располагаются на кристалле. Срезы, в свою очередь, состоят из справочных таблиц (look-up tables) и триггеров (flip flops). Количество справочных таблиц и триггеров, которые Xilinx определяет для создания одного среза, различается в зависимости от семейства кристалла. Кристалл XC7A200T имеет 134600 срезов. Измерения количества использованных срезов для устройств с количеством входов 4, 8, 16, 32, 64 отмечены точками (рисунок 2). Методом степенной регрессии получен график ожидаемой зависимости количества использованных срезов, от количества входных сигналов.

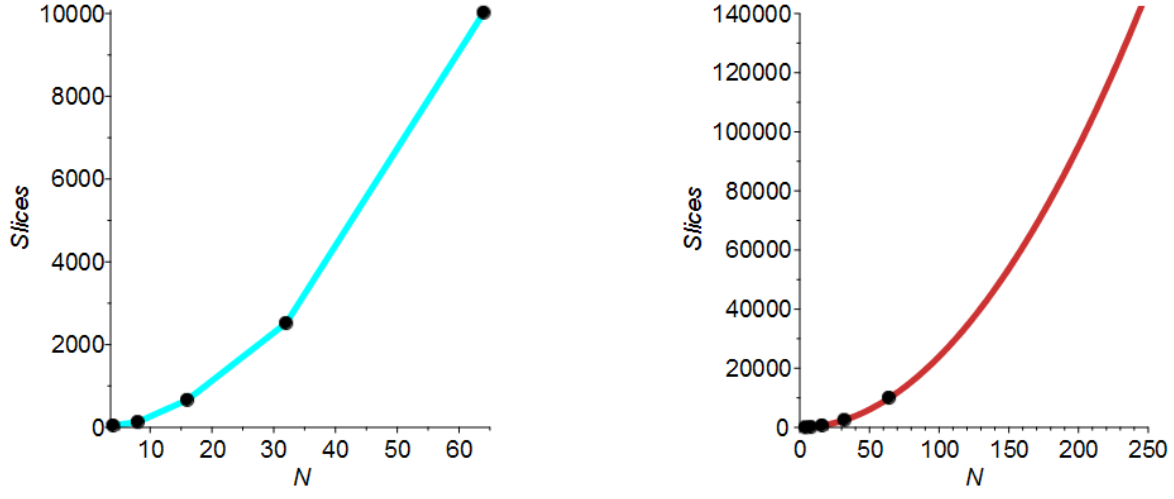

Рисунок 2. Практическая зависимость использованного количества срезов от количества входных сигналов (а), теоритическая зависимость использованного количества срезов от количества входных сигналов (б)

Согласно полученному уравнению регрессии, максимальная ожидаемая размерность устройства, которое можно разместить на кристалле XC7A200T, составляет N = 238. Также интерес представляет такой параметр, как частота [3]. Опытным путём было замечено, что с возрастанием размерности устройства, частота снижается (рисунок 3).

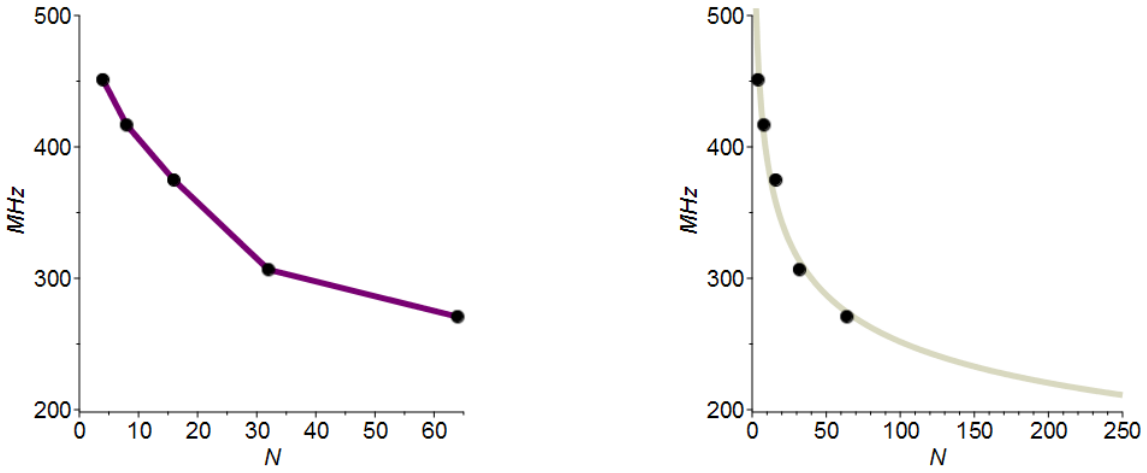

Рисунок 3. Практическая зависимость частоты от количества входных сигналов (а), теоритическая зависимость частоты от количества входных сигналов (б)

Результатом данной работы является приведённая оценка аппаратных затрат для изготовления цифрового устройства всевозможных перестановок. Так как кристаллы серии Artix-7 обладают относительно невысокой ценой, уменьшенным энергопотреблением по сравнению с предыдущими семействами, их использование вполне оправдано для массового производства цифровых устройств. Устройства могут использоваться для усложнения задач обратного проектирования систем как малой, так и относительно большой сложности. Однако следует учитывать, что увеличение количества входных сигналов ведёт не только к потере производительности, но и сильно ограничено сверху. Ограничения можно расширить, используя кристаллы большей ресурсоёмкости, тем не менее это приведёт к росту цены конечного продукта.

Список использованных источников:

1. Кохновский, С. И. Методика проектирования комбинационного устройства всевозможных перестановок [Электронный ресурс] / С. И. Кохновский // Компьютерные системы и сети : сб. тезисов докладов. – БГУИР, Минск, 2019. – 287 с. – С. 205-207. – Режим доступа: https://www.bsuir.by/m/12_100229_1_136895.pdf. – Дата доступа: 22.03.2020.

2. Artix-7 Product Advantage [Electronic resource]. – Mode of access: https://www.xilinx.com/products/silicon-devices/fpga/artix-7.html. – Date of access: 22.03.2020.

3. Clock Signals in FPGA Design: Data Path Maximal Clock Rates and the Xilinx PERIOD Timing Constraint [Electronic resource]. – Mode of access: https://www.allaboutcircuits.com/technical-articles/clock-signal-FPGA-design-clock-rate-xilinx-period-timing-constraint/. – Date of access: 22.03.2020.