ИССЛЕДОВАНИЕ РАСПРОСТРАНЕНИЯ СИГНАЛОВ НА ПАРАМЕТРИЧЕСКОЙ МОДЕЛИ ФНФ ТИПА АРБИТР

Шамына А.Ю.

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

Иванюк А.А. – д-р. техн. наук, профессор

В настоящей работе рассмотрено построение параметрической модели физически неклонируемой функции типа арбитр (АФНФ) средствами САПР Xilinx 14.7. Описана постановка эксперимента по временной оценке асимметрии прохождения копий тестового сигнала на различных звеньях блока симметричных путей (БСП) АФНФ, а также произведен анализ полученных результатов.

Существующие реализации АФНФ базируются на уникальности трансляции тестовых сигналов через БСП для каждого изделия [1]. Уникальность распространения тестовых сигналов через БСП АФНФ обусловлена различными инерциальными задержками коммутационных звеньев и транспортными задержками между ними. Однако в большинстве работ оценка асимметрии тестовых сигналов производится на выходах последнего узла БСП либо на арбитре, что затрудняет определение удельного вклада каждого звена БСП в конечный результат. Также остается открытым вопрос оценки доли вклада в общую энтропию инерциальных и транспортных задержек.

Для изучения АФНФ была создана параметрическая модель «Post place & route» с использованием САПР Xilinx 14.7 и HDL языка Verilog. Тестовые модули были описаны также на Verilog. Благодаря параметризации количества звеньев БСП созданная модель может быть применена для АФНФ различной размерности. Модель строилась для FPGA Xilinx Artix 7. При имплементации проекта была отключена логическая оптимизация, т.к. иначе после технологического синтеза каскад мультиплексоров БСП может быть отличным от ожидаемого.

Как правило, звено БСП имеет 3 входа (2 для тестовых сигналов и 1 для разряда запроса) и 2 выхода. В рамках реализации АФНФ на FPGA звено БСП состоит из двух lut-компонентов. Входы «a» и «b» являются входами тестовых сигналов, вход «c» представляет разряд запроса к АФНФ, а «x» и «y» являются выходами тестовых сигналов из звена БСП. На рисунке 1 представлен результат технологического синтеза звена БСП.

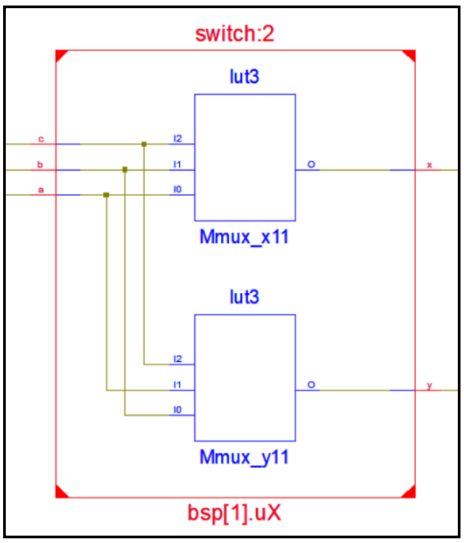

Рисунок 1 – технологический синтез звена БСП

В работе [2] модельные эксперименты проводились с учетом асимметрии входных сигналов на входах первого звена БСП. Использование языка Verilog при описании тестовых модулей позволило устранить эту асимметрию благодаря возможности установки значений внутренних сигналов тестируемого модуля напрямую. Также использование Verilog открыло возможность оценки временной асимметрии фронтов тестовых сигналов на выходах каждого звена БСП. Эта возможность позволяет за один запуск модельного эксперимента оценить временные разницы между фронтами при различном количестве звеньев БСП.

На временной диаграмме сигналов звена БСП (рисунок 2) можно проследить характерную асимметрию фронтов тестовых сигналов на выходах из звена, несмотря на полную симметричность сигналов на входах. Эта разница обусловлена внутренней асимметричностью путей сигналов, а также инерционностью коммутационных блоков. Для выбранного звена асимметричность на выходах составила 407 пс при прямой трансляции сигналов внутри блока и 63 пс при перекрестной соответственно.

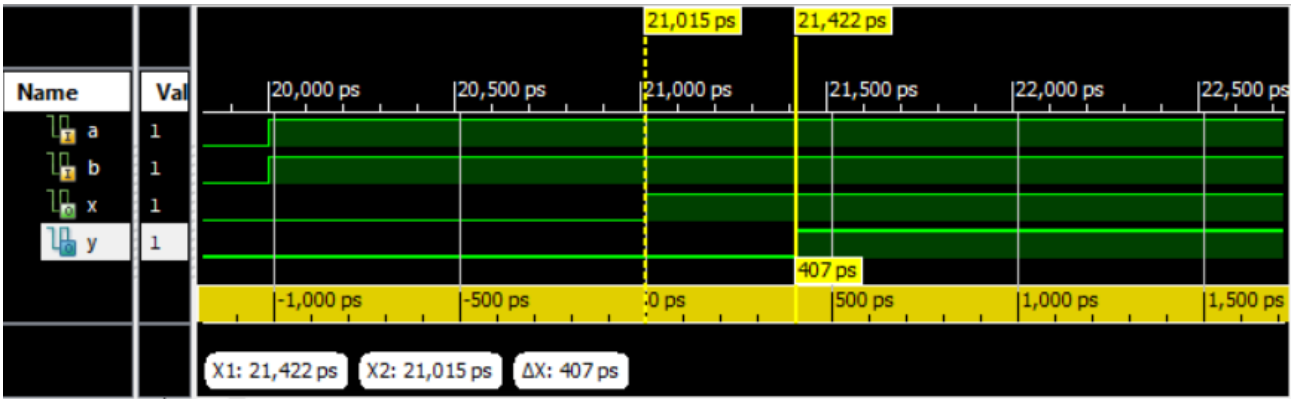

Рисунок 2 – временная диаграмма сигналов звена БСП

При проведении модельного эксперимента были сгенерированы все возможные запросы при разрядности 16. Для каждого запроса оценена временная асимметричность прохождения фронтов сигналов на выходах последнего звена БСП. Для анализа плотности временного распределения оценок асимметричности диапазон полученных значений был разбит на интервалы и осуществлен подсчет вхождений результатов в эти интервалы. Полученный результат представлен в виде гистограммы на рисунке 3

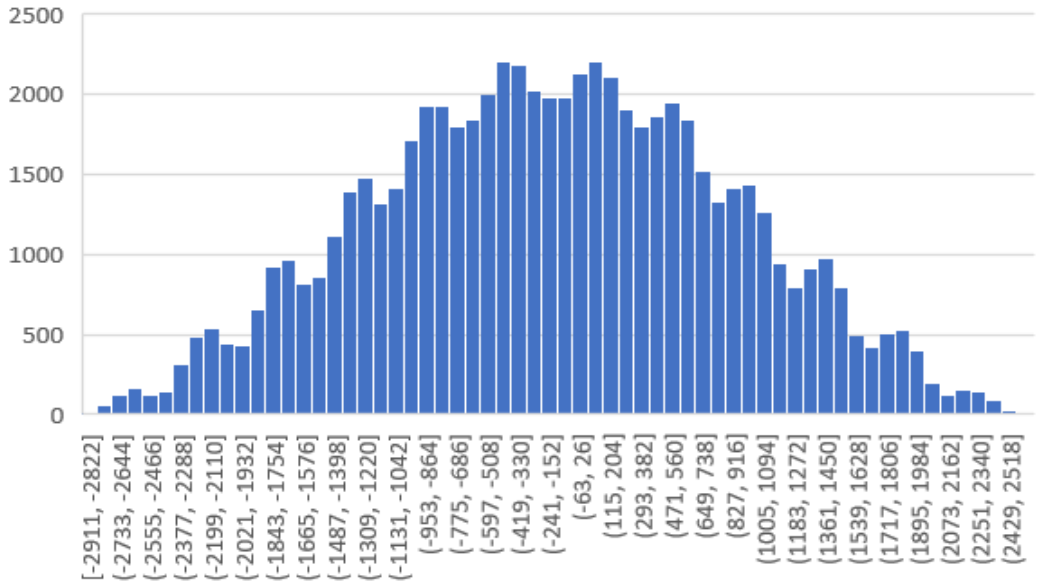

Рисунок 3 – гистограмма временных разниц фронтов сигнала на различных интервалах

Из рисунка 3 видно, что большинство результатов сосредоточено в потенциально метастабильном регионе (когда временная разница между фронтами тестовых сигналов близка к 0). Это может негативно сказаться на характеристиках ФНФ и потребовать применения дополнительных решений.

Список использованных источников:

. 1. Заливако, С. С. Физически неклонируемые функции / Заливако С. С., Иванюк А. А. // Информационные технологии и системы 2019 (ИТС 2019) = Information Technologies and Systems 2019 (ITS 2019) : материалы международной научной конференции, Минск, 30 октября 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2019. – С. 8 – 21.

2. Шамына, А. Ю. Анализ симметричных путей физически неклонируемой функции на FPGA / Шамына А. Ю., Иванюк А. А. // Информационные технологии и системы 2019 (ИТС 2019) = Information Technologies and Systems 2019 (ITS 2019) : материалы международной научной конференции, Минск, 30 октября 2019 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2019. – С. 150 – 151.