АНАЛИЗ СИММЕТРИЧНЫХ ПУТЕЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ НА FPGA

Шамына А. Ю., Иванюк А. А.
Кафедра программного обеспечения информационных технологий, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: shamyna@bsuir.by, ivaniuk@bsuir.by

Известные варианты реализации физически неклонируемой функции (ФНФ) типа арбитр базируются на синтезе конфигурируемых симметричный путей, обеспечивающих уникальную трансляцию тестовых сигналов для каждого изделия. В настоящей статье производится анализ зависимости основных характеристик ФНФ от количества структурных элементов блока симметричных путей (БСП) без учета влияния схемы арбитра на полученные результаты.

Введение

Для защиты цифровых устройств от нелегального копирования, а также для реализации генераторов случайных числовых последовательностей и других практических приложений широко используются ФНФ. Формально любую ФНФ можно описать как функцию $PUF(C) = R$, где C определяет множество запросов, а R – множество ответов [1]. Однако такие характеристики ФНФ, как уникальность и случайность, не являются идеальными, что заставляет искать новые способы улучшения этих свойств. Важнейшим критерием оценки стабильности ФНФ является ее устойчивость к изменениям внешних условий и сохранение собственных свойств с течением времени. С этой точки зрения представляет интерес для изучения ФНФ типа арбитр [2,3]. Наибольшее влияние на основные для данного типа ФНФ свойства оказывает БСП. В проведенной работе изучено влияние количества звеньев БСП на прохождение тестовых сигналов через него, дана оценка зависимости от этого конечных свойств ФНФ.

I. Реализация ФНФ типа арбитр и ее параметрической модели

Классическая реализация ФНФ типа арбитр подразумевает наличие трех последовательно соединенных составных компонентов (рисунок 1): генератора тестовых сигналов (ГТС), блока симметричных путей и арбитра. БСП состоит из N узлов, каждый из которых имеет два входа для тестового сигнала, один управляющий вход, соотвествующий одному разряду запроса и два выхода тестового сигнала. Значением сигнала с управляющего входа возможно определение двух конфигураций передачи тестового сигнала через звено БСП: прямой и перекрестной. При N звеньях возможны 2^n различных реализаций двух симметричных путей, что характеризует данную ФНФ как сильную.

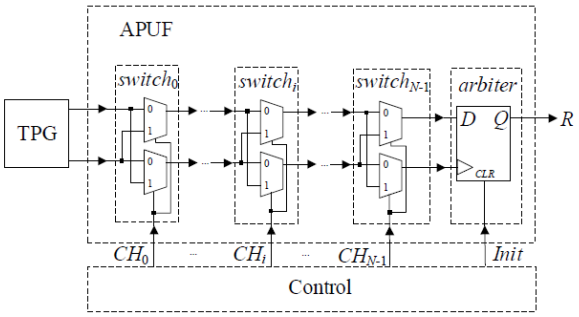

Рис. 1 – Структурная схема ФНФ типа арбитр

Было реализовано несколько вариантов ФНФ типа арбитр с различным числом структурных звеньев в БСП. Схемы ФНФ и тестовые модули были созданы на языке VHDL с использованием САПР Xilinx ISE 14.7. Параметрическая модель устройства была создана средствами САПР с учетом взаимного расположения и индивидуальных задержек элементов на кристалле FPGA Xilinx Artix-7. Отдельно следует отметить, что для генерации псевдослучайных тестовых последовательностей использовался LFSR с примитивным порождающим полиномом, степень которого соотвествует требуемой разрядности запроса. LFSR был реализован функционально в testbench-компоненте для исключения влияния схемы LFSR на результаты моделирования.

II. Оценка прохождения тестовых сигналов через БСП

Ключевой характеристикой ФНФ типа арбитр является разница между фронтами тестовых сигналов на выходах последнего узла БСП. Моделирование работы тестовых схем производилось с использованием симулятора ISE Simulator. Исследование было выполнено для моделей ФНФ с различным числом звеньев БСП ($N = 8$, $N = 16$, $N = 32$). Для $N = 8$ и $N = 16$ осуществлялся полный перебор возможных значений запроса ФНФ (2^8 и 2^{16} соответственно). Из-за высокой сложности полного пе-

ребора тестовых векторов для схемы с $N = 32$ в качестве генератора М-последовательности был выбран LFSR, с использованием которого было сгенерировано 2^{16} тестовых запросов. На рисунке 2 изображены три графика отсортированных по возрастанию значений временных разниц, наблюдаемых на выходах схемы БСП для трех реализаций: $N = 8$, $N = 16$ и $N = 32$ звеньев БСП. На оси абсцисс представлены не сами значения запросов, а их порядковые номера C_{index}. Выходы последнего звена БСП обозначены как x_{n-1} и y_{n-1}. Отрицательные значения $\Delta(x_{n-1}, y_{n-1})$ на графиках означают, что фронт тестового сигнала с выхода x_{n-1} пришел раньше, чем с выхода y_{n-1}.

Графики значений $\Delta(x_{n-1}, y_{n-1})$ для БСП $N = 32$ являются более симметричными относительно двух координатных осей. Кроме того, большие абсолютные значения разниц прохождения фронтов являются более предпочтительными, т.к. в случае использования в качестве арбитра последовательностных схем минимальная разница чревата переходом арбитра в метастабильное состояние и, как следствие, меньшей стабильностью ФНФ. Обусловлено это тем, что при большем числе звеньев БСП увеличивается длина симметричных путей. Также был выполнен частотный анализ более быстрого прохождения каждой из копий тестового сигнала. Так, при $N = 32$ частота более быстрого появления фронта тестового сигнала на выходе x_{n-1} примерна равна этой же величине для выхода y_{n-1} (0.49 и 0.51 соответственно). В то время как для схем с меньшим N ($N = 8$ и $N = 16$) характерна большая асимметрия этих значений: при $N = 16$ (0.4 и 0.6) и при $N = 8$ (0.45 и 0.55). Диапазоны результирующих значений $\Delta(x_{n-1}, y_{n-1})$ при меньшем N также обладают большей асимметрий относительно нулевого значения. При $N = 32$ диапазон равен [-10665;10300] пс, а для $N = 8$ и $N = 16$ составляет [-1757; 1561] пс и [-2720; 2210] пс соответственно. Важным преимуществом реализации ФНФ типа арбитр является минимальное число околонулевых значений разниц прохождения фронтов тестового сигнала, что выражается меньшей пологостью графика относительно оси абсцисс. Как видно из рисунка 2, наименьшее число околонулевых значений $\Delta(x_{n-1}, y_{n-1})$ характерно для $N = 32$.

III. Заключение

В ходе проведенной работы были изучены зависимости основных характеристик ФНФ от количества структурных элементов блока симметричных путей без учета влияния схемы арбитра на полученные результаты. Моделирование осуществлялось с использованием параметрических моделей ФНФ типа арбитр с различным числом звеньев в БСП. Из полученных в данной работе результатов можно сделать вывод, что наиболее целесообразным является использование ФНФ типа арбитр с большим числом звеньев БСП, т.к. увеличение их количества улучшает характеристики ФНФ, такие как стабильность, уникальность и случайность. Однако полученные результаты нуждаются в многократной верификации на реальном оборудовании.

Список литературы

1. Secure System Design and Trustable Computing / Springer; editors Ch.-H. Chang, M. Potkonjak. -– Switzerland, 2016. — p.537.
2. Иванюк, А. А. Особенности реализации симметричных путей ФНФ типа арбитр на ПЛИС / А. А. Иванюк // Информационные технологии и системы 2018 (ИТС 2018) = Information Technologies and Systems 2018 (ITS 2018) : материалы международной научной конференции, Минск, 25 октября 2018 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2018. – С. 156 - 157.
3. Заливако, С. С. Метод увеличения стабильности физически неклонируемой функции типа “арбитр” / С. С. Заливако, А. А. Иванюк, В. П. Клыбик // Информатика. – 2017. – №1(53). – С. 31 – 43.

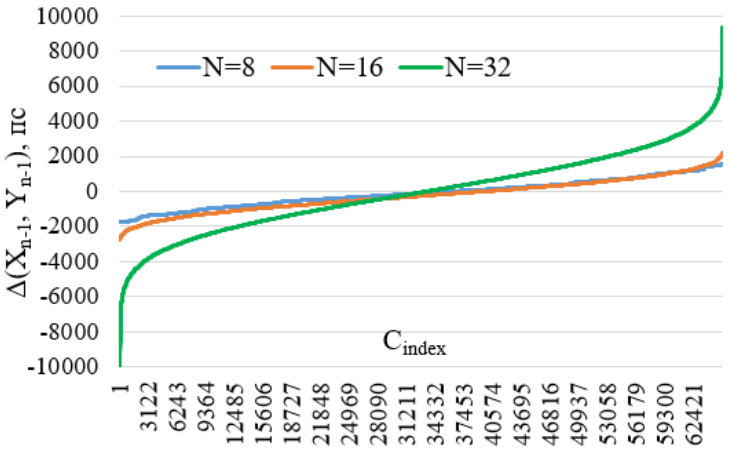

Рис. 2 – Графики значений $\Delta(x_{n-1}, y_{n-1})$ для различных реалзиаций БСП