ОСОБЕННОСТИ РЕАЛИЗАЦИИ СИММЕТРИЧНЫХ ПУТЕЙ ФНФ ТИПА АРБИТР НА ПЛИС

Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: ivaniuk@bsuir.by

Предложена новая архитектура звеньев симметричных путей для физической неклонируемой функции типа арбитр, позволяющая эффективно использовать аппаратные ресурсы программируемых логических интегральных схем. Показана практическая возможность реализации звеньев симметричных путей на внутренних ресурсах LUT-блоков на примере кристалла FPGA Xilinx Artix-7.

Введение

Физически неклонирунмые функции (ФНФ) являются объектами пристального внимания как со стороны научного сообщества, так и со стороны компаний-производителей цифровых устройств и систем, в основном благодаря своим основным свойствам *неклонируемости* и *случайности*. Формально произвольную ФНФ можно описать как функцию $PUF(C) = R$, где C определяет множество запросов, а R – множество ответов [1]. Для конкретной реализации ФНФ уникальным и случайным является множество пар запрос-ответ $CR = \{C, R\}$. При этом конктерные значения CR являются случайными и *неуправляемыми*, и становятся известными только после изготовления цифрового устройства либо системы. Реализация идентичной системы (*клонирование*) приведет к получению нового множества $CR^* \neq CR$. Для усиления свойств неклонируемости и случайности множество пар CR должно быть достаточно большим и выбирается исходя из практической недостижимости получения значений всех возможных пар. Например, для ФНФ с $N = 128$ входами двоичных значений запросов C мощность множества CR составляет 2^{128}, что делает практически недостижимым их получение, хранение и последующий анализ. Подобные ФНФ называются *сильными* ФНФ, которым приписывают еще одно важное свойство *непредсказуемости*, заключающееся в невозможности определения (прогнозирования) значения конктерной пары $\{C_i, R_i\}$ при известном значении $\{C_j, R_j\}$, $i \neq j$, $i, j \in [0, 2^N - 1]$.

Описанные выше свойства ФНФ применяются для реализации неклонируемой идентификации/аутентификации интегральных схем и реализованных на них цифровых устройств, для построения генераторов случайных невоспроизводимых числовых последовательностей, для реализации аппаратных хэш-функций и др. [1].

Однако практическое применение ФНФ сталкивается с рядом проблем, среди которых основной является проблема повторяемости пар CR во времени. Данное свойство определяется такой характеристикой ФНФ как *стабильность*, значение которой зависит от таких факторов как температура окружающей среды, значение питающего напряжение, степень износа кристалла интегральной схемы и др. Кроме этого такие характеристики ФНФ как уникальность и случайность также являются не идеальными, что заставляет исследователей и разработчиков искать новые методы их улучшения [1].

В данной работе предлагается новая архитектура сильной ФНФ типа арбитр, позволяющая более эффективно использовать имеющиеся конфигурируемые ресурсы ПЛИС. В отличии от существующих архитектур предлагаемая архитектура характеризуется наличием множественных локальных симметричных путей, принципиально неуправляемых со стороны разработчика.

I. ФНФ типа арбитр

Схемотехническая реализация ФНФ типа арбитр представляет собой цифровое устройство, включающее в себя следующие основные компоненты: генератор тестового сигнала (ГТС), блок симметричных путей (БСП), состоящий из N симметричных звеньев, и собственно арбитра. Каждое звено имеет два входа для тестового сигнала, один управляющий вход и два выхода, последовательно соединенные с предыдущим и последующим звеном. Таким образом последовательно соединенные N звеньев образуют БСП. Управляющий вход каждого i-го звена соединен с соответствующим входом запроса C_i, значение которого определяет одну из двух возможных конфигураций: $C_i = 0$ – прямая передача значений сигналов со входов звена на соответствующие два выхода и $C_i = 1$ – перекрестная передача значений сигналов. Для N последовательно соединенных звеньев количество возможных комбинаций оценивается как 2^N, что характеризует ФНФ типа арбитр как сильную ФНФ. Два выхода последнего звена, управляемого сигналом запроса C_{N-1}, поступают на схему арбитра, который оценивает какая из копий тестового сигнала от ГТС пришла первой на заданной конфигурации БСП. ФНФ типа арбитр хорошо исследована и апробирована на различных технологиях, в том числе и на кристаллах ПЛИС. Она

обладает достаточной стойкостью к температурным воздействиям, что делает ее пригодной к построению стабильных неклонируемых идентификаторов [1].

При реализации ФНФ типа арбитр на ПЛИС основная доля аппаратурных затрат приходится на имплементацию БСП. В общем случае для реализации одного звена необходимо два двухвходовых мультиплексора с перекрестным соединением входных портов. Технологическая схема реализации одного звена на ПЛИС требует наличия двух аппаратных LUT-блоков, а именно LUT-3, для которых использованы три логических входа: два для тестового сигнала и один для сигнала запроса. Обобщая вышесказанное можно утверждать, что для реализации БСП длины N на ПЛИС необходимо использование $2N$ LUT-3 технологических блоков.

Наряду с описанными достоинствами ФНФ типа арбитр обладает и рядом недостатков, среди которых можно отменить имеющуюся линейную зависимость множеств запросов и формируемых на них ответов, позволяющую достаточно эффективно применять методы машинного обучения с целью построения точной программной модели такой ФНФ. Эффективными методами, затрудняющими атаки на ФНФ при помощи машинного обучения, являются архитектурные методы, увеличивающие множество симметричных путей и нелинейные преобразования над множеством запросов и ответов. Это, в свою очередь, приводит к увеличению аппаратных затрат с неэффективным использование ресурсов ПЛИС.

Современные ПЛИС типа FPGA имеют в своем составе LUT-блоки, позволяющие реализовывать произвольные комбинационные схемы с большим числом входов. Например, FPGA фирмы Xilinx семейства Artix-7 имеет LUT-блоки с шестью входами [2]. В случае реализации одного звена БСП на Artix-7 только три входа из шести LUT-6 блока будут использованы, и будет задействована только $1/8$ памяти конфигурации этого же блока.

II. Предлагаемая архитектура ФНФ типа арбитр

В данной работе предлагается новая архитектура симметричных путей ФНФ типа арбитр с учетом их реализации с использованием технологических примитивов LUT-6. Для k входов копий тестового сигнала необходимо наличие $\lceil log_2 k \rceil$ адресных входов для реализации мультиплексирования сигнала с выбранного входа на единственный выход. Таким образом для LUT-6 блока имеем следующее неравенство $k + \lceil log_2 k \rceil \leq 6$. Одним из решений данного неравенства является значение $k = 4$. Таким образом, реализация одного полноценного звена с использованием двух блоков LUT-6 позволяет реализовать четыре конфигурации симметричных путей. Данный подход, в отличие от классической архитектуры, позволяет полностью использовать аппаратные ресурсы LUT-блоков как по числу входов, так и по памяти конфигурации. Если реализация классической схемы ФНФ типа арбитр на FPGA семейства Artix-7 использует $2N$ LUT-6, то предлагаемая архитектура позволяет реализовать ФНФ с большим числом входов при использовании той же аппаратуры.

III. Анализ основных характеристик

Внутренняя структура блока LUT-6 включает в себя 64-разрядный регистр конфигурации и 63 двухвходовых мультиплексора, формирующие древовидную 6-уровневую схему выборки. По предложенной архитектуре все возможные четыре конфигурации внутри блока LUT-6 формируют локальные симметричные пути прохождения тестового сигнала до единственного выхода. Согласно основному свойству ФНФ все пути в конкретном блоке LUT-6 имеют различные задержки распространения сигнала. Ниже представлены данные о задержках, полученные путем параметрического моделирования VHDL-модели различных звеньев ФНФ типа арбитр, реализованных на различных LUT-блоках кристалла FPGA Artix-7 XC7A100T (CSG324).

Таблица 1 – Значения задержек распространения сигналов для трех различных блоков LUT-6, (ns)

Запрос	LUT-6(1)	LUT-6(2)	LUT-6(3)
00	0,897	0,847	0,838
01	1,023	0,999	0,979
10	0,858	0,927	0,907
11	1,103	1,071	1,044

IV. Заключение

Предложена новая архитектура блока симметричных путей для ФНФ типа арбитр, позволяющая экономично использовать внутренние ресурсы ПЛИС типа FPGA. Благодаря использованию локальной неуправляемой симметрии внутренних путей аппаратных LUT-блоков зависимость множества ответов от множества запросов усложняется, что потенциально затрудняет применение атак на данный тип ФНФ с помощью методов машинного обучения.

V. Список литературы

1. Secure System Design and Trustable Computing / Springer; editors Ch.-H. Chang, M. Potkonjak. -– Switzerland, 2016. — p.537.
2. 7 Series FPGAs Configurable Logic Block, User Guide [Electronic resource] / Xilinx Inc., 2016. – Mode of access: https://www.xilinx.com/. – Date of access: 08.10.2018.