ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ОСНОВНЫХ ХАРАКТЕРИСТИК МУЛЬТИАРБИТРАЛЬНОЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ

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

Пучков А. В.

Иванюк А. А. – доктор технических наук, профессор

Одной из важнейших проблем, решаемых в рамках проектирования современных цифровых устройств, в том числе реализуемых на базе программируемых логических интегральных схем, на текущем этапе развития технологий и рынка, является их идентификация. Перспективным направлением решения указанной проблемы является применение так называемых физически неклонируемых функций. Являющееся предметом работы экспериментальное исследование позволяет сделать выводы о возможности и эффективности решения задачи идентификации с помощью мультиарбитральной физически неклонируемой функции для цифровых устройств на основе программируемой логики.

Методы физической криптографии, в основе которой лежит структурная сложность электронных систем, всё чаще находят применение в области защиты цифровых систем от нелегального использования [1]. Согласно одному из современных формальных определений, которое было предложено П. Туилсом (P. Tuyls), физически неклонируемая функция (ФНФ, англ. Physically Unclonable Function, PUF) понимается как характеристика физической (цифровой) системы, которая не подлежит клонированию (копированию, воспроизведению) на других системах [2]. В процессе создания цифровых устройств и систем принципиально невозможно управлять величинами многих физических параметров, вследствие чего последние из-за физической вариации технологического процесса принимают случайные, но уникальные для каждой цифровой системы значения. Принцип извлечения подобных уникальных параметров из цифровых систем и лежит в основе аппаратных реализаций ФНФ [1].

Задача ФНФ как цифрового устройства состоит в получении на выходных портах множества ответов R, соответствующих множеству запросов C таким образом, что пары $(C_i, R_i), C_i \in C, R_i \in R$ будут уникальными, непредсказуемыми и неклонируемыми на других аналогичных интегральных схемах, в том числе и произведённых одновременно [3]. Такие свойства позволяют успешно использовать ФНФ для решения целого ряда задач, к которым в первую очередь относится уникальная идентификация цифровых систем.

В основе структуры и функционирования многих ФНФ является измерение инерциальных и транспортных задержек сигналов в реконфигурируемых путях цифровых устройств. Классическим примером такого подхода является ФНФ типа арбитр, когда на одном кристалле интегральной схемы выполняется построение двух топологически и функционально идентичных путей, которые имеют близкие, но принципиально различные из-за физической вариации технологического процесса, величины времени распространения сигналов по ним. Симметричные пути проектируются как пары двухвходовых мультиплексоров, селективные входы которых образуют шину входных запросов ФНФ. Измерение разницы во времени распространения сигналов между двумя путями может быть осуществлено одновременной подачей фронта импульса и определением на выходах, какой из них оказался длиннее [1]. Последнее может в простейшем случае быть достигнуто при помощи синхронного D-триггера, сбрасываемого в нуль до выполнения измерений. В этом случае один из путей подаётся на вход данных триггера, а другой – на его вход синхронизации. Легко показать, что в данном случае ответ, регистрируемый на выходе триггера, показывает, какой из путей имеет большую задержку распространения сигнала.

Объектом рассматриваемого экспериментального исследования была выбрана принципиально модифицированная схема, основанная на классической реализации ФНФ типа арбитр – мультиарбитральная ФНФ (рис. 1), характерной чертой которой являются арбитры, подключенные к каждому звену симметричных путей. Выбор одного из сигналов ответов осуществляется с помощью мультиплексора [3].

Данная реализация является очень гибкой и позволяет провести оценку разрешающей способности ФНФ при идентификации цифровых устройств в рамках отдельной системы на кристалле. Следует отметить, что в случае программируемых логических интегральных схем весьма сложно добиться симметричности всех путей, вследствие чего можно с достаточной точностью говорить о существовании непустого подмножества путей, являющихся ассиметричными. Важно также, что вследствие нарушения величин времени установления и удержания, возможен переход триггера в метастабильное состояние, что соответствует значению X типа std_logic языка VHDL. Регистрация подобных явлений на реальных аппаратных средствах сопряжена с определёнными трудностями. В рамках данного исследования использовано многократное измерение ответов ФНФ с дальнейшим усреднением. Тогда критерием, устанавливающим соответствие усреднённого значения ответа с алфавитом $\{0,1,X\}$, является принадлежность интервалам $(0;0{,}4),(0{,}4;0{,}6),(0{,}6;1)$ для 0, X и 1 соответственно. Поскольку анализ ответов с возможными значениями X значительно усложняется по сравнению с бинарным случаем, было использование преобразование к двоичным парам ответов, соответствующее минимальности метрики различия (наихудшему случаю с точки зрения качества идентификатора).

Библиотека БГУИР

С целью оценки качества полученных идентификаторов была использована специальная метрика различия бинарных векторов. Пусть a, b, c, d – число компонент векторов 11, 01, 10, 11 соответственно. Тогда характеристика различия может быть представлена следующим образом:

$$D = \big(P_{01}(v_1) + P_{01}(v_2)\big)D_{SM} = \frac{1}{m^2}(b+c)(\min(a+c, b+d) + \min(a+b, c+d)),$$

где $P_{01}(v_\text{i})$ – характеристика случайности вектора v_i, D_{SM} – расстояние Сокала-Михенера.

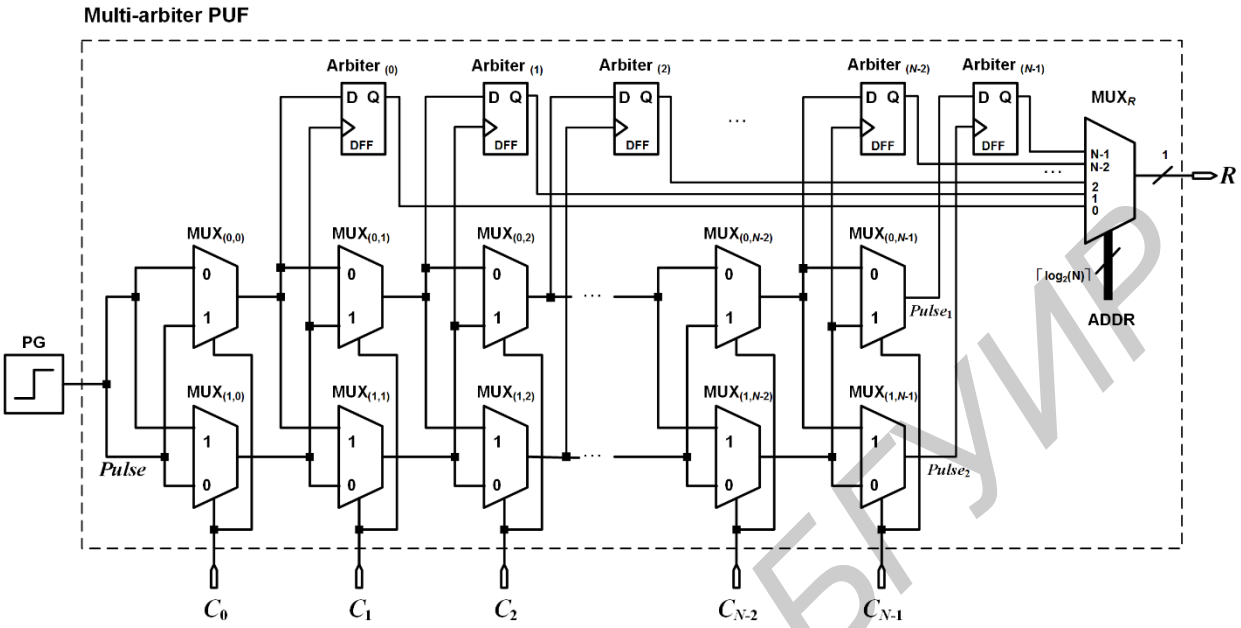

Рис. 1 – Функциональная схема мультиарбитральной PUF [3]

Для реализации мультиарбитральной ФНФ в рамках рассматриваемого экспериментального исследования были выбраны программируемые логические интегральные схемы типа FPGA Xilinx Spartan-3E XC3S500E-5FG320, представленные платами быстрого прототипирования Digilent Nexys 2. Для данной серии FPGA были разработаны проектные описания на языке VHDL мультиарбитральной ФНФ, контроллера, генераторов входных запросов, а также интерфейсного модуля, осуществляющего взаимодействие с рабочей станцией.

В качестве генераторов входных запросов были выбраны двоичный счётчик и генератор псевдослучайной последовательности на сдвиговом регистре с линейной обратной связью (LFSR) длиной 128 на основе порождающего полинома $x^{128} + x^{126} + x^{101} + x^{99} + 1$. Для ослабления корреляционной зависимости, присущей данному типу генераторов, генерация следующего запроса производилась через 128 тактов сигнала синхронизации.

Характеристиками, подлежащими анализу, являются вероятность появления значения X на различных арбитрах, представленная в виде гистограммы, значения метрики D в зависимости от номера арбитра, а также минимальные значения указанных величин. Совершенно необходимым является эксперимент по проведению идентификации экземпляров ФНФ минимальным возможным количеством запросов.

В ходе первичных исследований была показана целесообразность и эффективность использования мультиарбитральной PUF для решения проблемы уникальной идентификации как внутри отдельно взятой интегральной схемы, так и между интегральными схемами.

Список использованных источников:

1. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем: монография / А. А. Иванюк. – Минск: Бестпринт, 2012. – 337 с.
2. Tuyls, P. Security with Noisy Data / P. Tuyls, B. Skoric, T. Kevenaar. – London: Springer, 2007. – 344 p.
3. Клыбик, В. П., Иванюк, А. А. Применение физически неклонируемой функции типа арбитр для решения задачи идентификации цифровых устройств. / В. П. Клыбик, А. А. Иванюк – Информатика, 2015. – в печати.

Библиотека БГУИР