АНАЛИЗ И ПАРАМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ АРБИТРА ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ

Клыбик В. П., Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: vold029@gmail.com, ivaniuk@bsuir.by

Рассматриваются особенности анализа параметрической модели арбитра физически неклонируемой функции при помощи различных продуктов программных симуляторов.

Введение

Физически неклонируемая функция (ФНФ) цифрового устройства может быть определена множеством пар запрос-ответ:

$$R_i = PUF(C_i) => PUF\{C_i; R_i\},$$

где R_i – ответ на запрос C_i, $\forall$ i = 0, 1, 2, ...

Основными свойствами ФНФ являются:

- невоспроизводимость математической/алгоритмической модели;
- некопируемость при тиражировании схемной реализации.

Основными применениями ФНФ являются:

- идентификация и аутентификация цифровых устройств;
- генерирование секретных ключей для криптографии;
- реализация аппаратных хэш-функций;

Методы идентификации, аутентификации, аппаратные хэш на основе ФНФ требуют стабильных пар запрос-ответ. В реалистичных реализациях наблюдаются нестабильные ответы при повторении одинакового запроса. Обусловлено это тепловым, электромагнитным шумом и другими факторами. Предлагаемый доклад посвящен исследованию ФНФ типа арбитр, где нестабильность ответов может быть вызвана особенностями сравниваемых путей и схемы арбитра применительно к технологиями ПЛИС, а именно FPGA.

I. ФНФ типа арбитр

Схема ФНФ состоит из генератора тестового импульса **PG**, двух симметричных путей длиной $\boldsymbol{n}$, реализованных на двухвходовых мультиплексорах **MUX**, и арбитра на синхронном D-триггере **DFF**.

Рассмотрим фазы последовательного функционирования:

1. На входах $\boldsymbol{C}$ устанавливается запрос, состоящий из набора сигналов $\boldsymbol{C_0 - C_{n-1}}$. По входному запросу мультиплексорами формируется пара симметричных путей прохождения тестового сигнала.
2. Генерируется тестовый импульс $\boldsymbol{S}$, который распространяется по двум сформированным симметричным путям. В результате на выходах путей мы получаем два тестовых импульса $\boldsymbol{S_1}$ и $\boldsymbol{S_2}$.
3. Тестовые импульсы $\boldsymbol{S_1}$ и $\boldsymbol{S_2}$ приходят на входы данных и синхронизации арбитра. Однако, ввиду девиации физических характеристик электронных элементов на кристалле, время распространения тестового сигнала по путям будет разным и фронты сигналов $\boldsymbol{S_1}$ и $\boldsymbol{S_2}$ не будут совпадать во времени. Если первым придет фронт сигнала $\boldsymbol{S_2}$, то на выходе арбитра мы получим $\boldsymbol{R = 0}$, иначе получим $\boldsymbol{R = 1}$.

В работах [1, 2, 3, 4] представлены результаты исследований схемных реализаций ФНФ для различных технологий, в том числе и для FPGA.

Для оценки и прогнозирования достоверности ФНФ типа арбитр первоочередной задачей является необходимость анализа временных характеристик симметричных путей и самого арбитра.

Для случая реализации ФНФ типа арбитр на базе FPGA, инструментальное измерение временных характеристик симметричных путей и арбитра крайне затруднено, ввиду сложности доступа к элементам кристалла. Для получения оценочных значений изучаемых временных характеристик было применено параметрическое моделирование и симуляция низкоуровневой схемной реализации ФНФ типа арбитр на FPGA при помощи специализированного программного обеспечения.

II. Параметрическое моделирование арбитра

Для создания и анализа параметрической модели ФНФ типа арбитр было использовано программное обеспечение Xilinx ISE. Полученная Post Place-Route модель, т.е. модель аппаратной схемной реализации на уровне размещения элементов на конкретном кристалле FPGA Xilinx SPARTAN-3E, была подвергнута параметрической симуляции в Xilinx ISIm. Полученные результаты позволили получить статистику реакции арбитра на входные воздействия для разных наборов сигналов. Однако, отсутствие наблюдаемости и управляемости внутренних полюсов моделируемой схемы в Xilinx ISIm симуляторе не позволило достоверно оце-

нить временные характеристики симметричных путей и арбитра, т.к. анализ временных значений сигналов на уровне выходных портов может отличаться на порядки от искомых внутрисхемных значений. Для получения необходимых временных значений внутрисхемных сигналов был использован альтернативный симулятор – ModelSim. ModelSim позволяет при описании и запуске блока тестирования (TestBench) использовать специальные функции **Signal_Spy** и **Signal_Force**, которые дают доступ к внутрисхемным сигналам, позволяя получить значение сигнала, либо, соответственно, принудительно установить его в нужное значение. Для выявления пороговых временных параметров схемы арбитра было создано специализированное TestBench-описание, которое путем последовательного приближения определило с точностью до 1 пикосекунды граничные значения времени реакции схемы арбитра на базе D-триггера на входные сигналы, аналогичные сигналам симметричных тестовых путей. Для ускорения работы приложения был использован алгоритм дихотомии при поиске конечного значения при последовательном приближении. На рисунке 1 представлен снимок экрана, полученный в результате симуляции, с измеренной разностью времени входных сигналов арбитра.

В таблице 1 представлены значения разности времени прихода тестовых сигналов арбитра, приводящее его к переходу в разные выходные состояния.

Таблица 1 – Пограничные состояния арбитра

Состояние арбитра	0	X	1
Разность времени, пс	<250	>249/<94	>93

Выводы

Исследование временных характеристик арбитра ФНФ на базе D-триггера показало чувствительность арбитра только к одному типу к относительного смещения временных параметров выходных тестовых сигналов симметричных линий. Эта особенность может отрицательно влиять на параметры достоверности ФНФ. Путем улучшения достоверности ФНФ, могут быть мультитриггерные реализации арбитров, использующие встречное, комбинированное и прочее включение тестовых входов компонентов арбитра, специальную логику формирования одинарного или векторного выходного сигнала арбитра.

План дальнейших исследований включает:

- Получение временных характеристик тестового сигнала на выходе симметричных тестовых путей для разных наборов данных
- сравнение результатов функциональной симуляции одинаковой Post Place-Route модели при помощи симуляторов ISIm и ModelSim на одинаковых наборах данных
- разработка методики проверки результатов, полученных в результате симуляции, на аппаратной реализации соответствующего кристалла FPGA
- моделирование и проверка эффективности мультитриггерных схемных реализаций арбитров ФНФ

1. Ozturk, E. Physical unclonable function with tristate buffers / E. Ozturk, G. Hammouri, B. Sunar // Circuits and Systems (ISCAS2008): Proc. of Int. Symp., Seatle, Washington, USA, 18-21 May 2008. – P. 3194-3197.
2. Hori, Y. Quantitative and Statistical Performance Evaluation of Arbiter Physical Unclonable Functions on FPGAs / Y. Hori, T. Yoshida, T. Katashita, A. Satoh // Research Center for Information Security[Electronic resource]. – Mode of access: http://staff.aist.go.jp/hori.y/articles/hori_reconfig2010.pdf. – Date of access: 11.08.2012.
3. Morozov, S. An Analysis of Delay Based PUF Implementations on FPGA / S. Morozov, A. Maiti, P. Schaumont // Virginia Tech Department of Electrical and Computer Engineering[Electronic resource]. – Mode of access : http://rijndael.ece.vt.edu/puf/paper/arc2010.pdf. – Date of access: 15.09.2012.
4. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – №2. – С. 90-100.

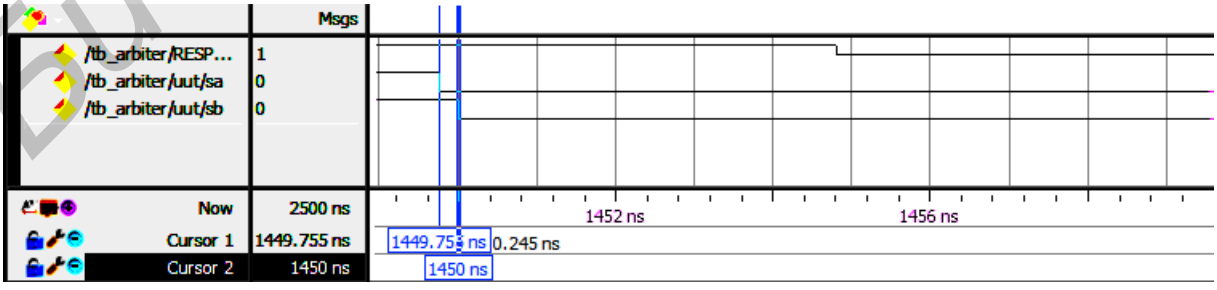

Рис. 1 – Результат симуляции в ModelSim