АНАЛИЗ И ПАРАМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ МУЛЬТИАРБИТРАЛЬНОЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ

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

Рассматривается новый вариант реализации физически неклонируемой функции типа арбитр. При помощи программной симуляции изучается влияние предлагаемых изменений на основные свойства физически неклонируемой функции.

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 цифровых устройств;
- генерирование криптографических ключей.

Идентификация при помощи ФНФ требуют стабильных пар запрос-ответ и различимость экземпляров устройств. В классических ФНФ типа арбитр наблюдаются нестабильные ответы при одинаковом запросе, что обусловлено разными факторами. Один бит ответа требует множества запросов для уверенной идентификации, что снижает число идентифицируемых устройств. Предлагаемый доклад посвящен исследованию новой реализации ФНФ типа арбитр. Исследования проводятся применительно к технологиями ПЛИС, а именно FPGA.

I. Реализация ФНФ типа арбитр

Классическая схема ФНФ и принципы ее функционирования были рассмотрены нами ранее в работе [1].

Известными недостатками описанной реализации являются нестабильные ответы при повторении одинакового запроса и относительно низкая разрешающая способность для идентификации экземпляров устройств.

Для улучшения указанных свойств, предлагается модификация ФНФ, изображенная на рис. 1, где арбитры установлены после каждого звена сравниваемых путей. Такой подход позволяет получить многобитовый ответ ФНФ на единичный запрос, что значительно увеличивает разрешающую способность ФНФ для идентификации и, предположительно, позволит всегда получать стабильную часть битового вектора ответа. Предлагается далее называть такую модификацию ФНФ цепочно-мультиарбитральной, либо просто мультиарбитральной.

Для исследования новой ФНФ было применено программное параметрическое моделирование низкоуровневой схемной реализации на FPGA.

II. Параметрическое моделирование мультиарбитральной ФНФ

Для создания и анализа параметрической модели было использовано программное обеспечение Xilinx ISE. Полученная Post Place-Route модель, т.е. модель аппаратной схемной реализации на уровне размещения элементов на кристалле FPGA Xilinx SPARTAN-3E, была подвергнута параметрической симуляции в пакете Mentor Graphics ModelSim. Результаты моделирования позволили получить статистику ответов ФНФ на входные воздействия для разных наборов сигналов, включая не только выходные значения 0 и 1, но и X – метастабильное состояние арбитров. Моделированию подверглись 10 мультиарбитральных ФНФ с длиной тестового пути 128 на одном кристалле FPGA.

III. Выводы

Параметрическое моделирование показало, что вне зависимости от расположения, с увеличением длины тестового пути:

- вероятность метастабильного состояния арбитра асимптотически стремиться к нулю, хотя на практике всегда от него отлична;
- распределение количества 0 и 1 в векторе ответа стремиться к идеальному 50/50.

Результаты моделирования показывают и минимальную длину тестового пути, которая имеет смысл для практической реализации с точки зрения получения адекватных ответов ФНФ для данного типа кристала и арбитров – 20. Графики результатов отображены на рис. 2.

Удельное расстояние по Хэммингу между парами ответов составило для всех ФНФ: среднее значение – 53,7, минимальное значение – 47,3,

что гипотетически показывает высокую разрешающую способность идентификации экземпляров устройств.

Использование вместо однобитного представления ответа битового вектора позволит существенно повысить достоверность идентификации, при сохранении высокой скорости формирования значения. Дополнительно, применение результатов статистического анализа ответов в качестве идентификаторов устройств, позволит гибко решать задачи аутентификации устройств с требуемым конкретной задачей уровнем достоверности, значительно повысив сложность анализа протоколов аутентификации злоумышленниками.

План дальнейших исследований включает: разработку тестовых реализаций цепочно-мультиарбитральной ФНФ для реальных аппаратных плат; исследование разрешающей способности мультиарбитральной ФНФ для идентификации экземпляра устройства; исследование диапазонов стабильности битовых векторов ответов мультиарбитральной ФНФ на реальных кристаллах.

1. Клыбик, В. П. Физически неклонируемые функции / В. П. Клыбик, А. А. Иванюк // Материалы международной научной конференции "ИТС 2013-– Минск: БГУИР, 2013. – С. 188-189.
2. 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.
3. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – №2. – С. 90-100.

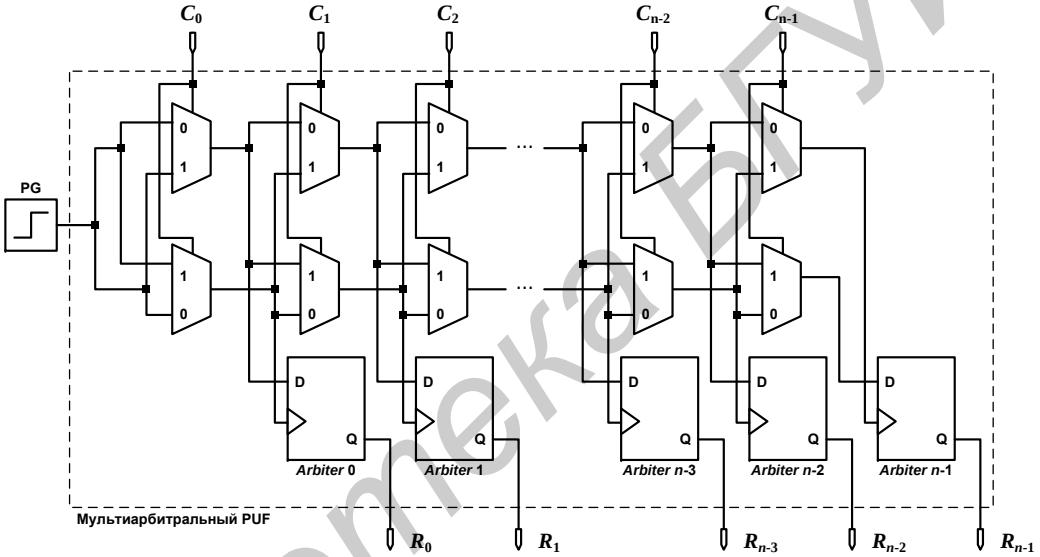

Рис. 1 – Схемная реализация мультиарбитральной ФНФ

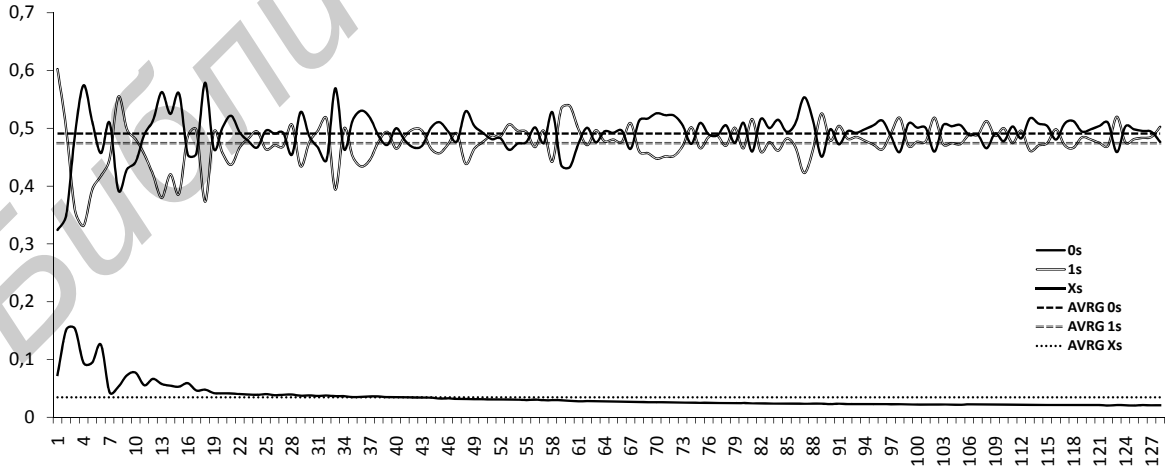

Рис. 2 – График распределения значений в ответах арбитров