В. П. Клыбик

ИССЛЕДОВАНИЕ ПАРАМЕТРИЧЕСКИХ МОДЕЛЕЙ АРБИТРОВ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Рассматривается анализ параметрических моделей разных схем арбитров физически неклонируемой функции. Предлагаются дальнейшие пути стабилизации нечетких ответов, регистрируемых на арбитрах.

Для задач идентификации устройств на FPGA используются физически неклонируемые функции (Physical Unclonable Function – PUF), работа которых основана на определении физических вариаций технологического процесса интегральных схем. Для достоверной идентификации важным параметром является стабильность PUF и арбитра PUF в частности. При этом, экспериментально доказано наличие нестабильности в ответах PUF [1]. Проведем анализ параметрических моделей разных схем арбитров PUF.

Рассмотрим технологию реализации PUF на FPGA, в частности на кристале Xilinx Spartan-3E. В качестве параметрических моделей использовались HDL-модели, полученные в САПР Xilinx ISE после выполненных процедур Place and Route.

Исследованию подвергались:

- минимальное время предустановки входных сигналов для различных моделей арбитров;
- время срабатывания арбитров;
- временные параметры симметричных путей PUF типа арбитр.

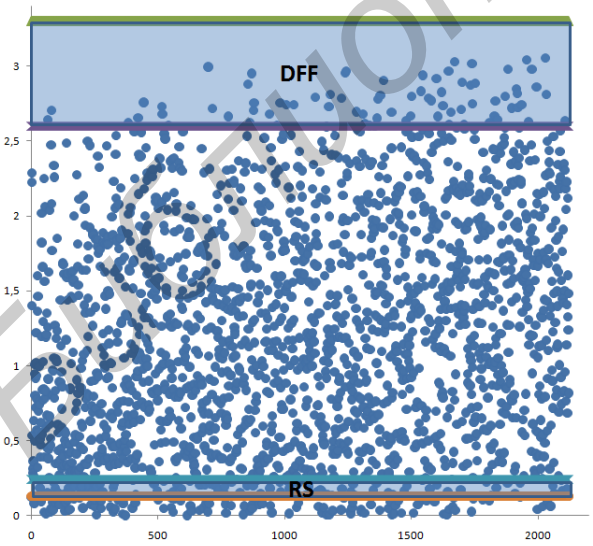

Рис. 1 – Частные результаты моделирования DFF и RS триггеров

График на рисунке 1 показывает распределение разности времени прохождения тестового импульса по параллельным путям на пространстве различных запросов для путей длиной 128 элементов. Верхняя зона на графике обозначает временную зону неопределенного состояния для арбитра на D-триггере, нижняя область - для RS-триггера.

Из результатов моделирования четко прослеживается:

- большинство запросов расположены ниже зоны адекватной работы D-триггера;
- большинство запросов расположены в зоне адекватной работы RS-триггера;
- наличие запросов ниже зоны адекватной работы RS-триггера;
- наличие запросов в зонах неопределенности триггера обоих типов.

Для получения адекватных результатов при проектировании и исследовании PUF типа арбитр необходимо знать и учитывать временные параметры функционирования конкретных схемных элементов. Для дальнейшей стабилизации PUF типа арбитр возможны следующие направления:

- анализ не только фронтов, но и спадов на выходе параллельных путей;
- использование мажоритарного арбитра;
- идентификация не за счет стабильности ответа PUF, а за счет статистического анализа нечетких ответов PUF.

1. Jouini, Z. C. Performance evaluation of Physically Unclonable Function by delay statistics. / Z. C. Jouini, J. -L. Danger, L. Bossuet // New Circuits and Systems Conference. –2011. P. 482–485.

Клыбик Владимир Петрович, аспирант кафедры вычислительных методов и программирования БГУИР, vold029@gmail.com.

Научный руководитель: Иванюк Александр Александрович, заведующий кафедрой вычислительных методов и программирования БГУИР, доктор технических наук, доцент, ivaniuk@bsuir.by.