АНАЛИЗ ХАРАКТЕРИСТИК ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ТИПА АРБИТР РАЗЛИЧНЫХ КОНФИГУРАЦИЙ

Шамына А. Ю., Иванюк А. А.
Кафедра программного обеспечения информационных технологий, кафедра информатики,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: {shamyna, ivaniuk}@bsuir.by

Произведен анализ характеристик случайности, уникальности и стабильности физически неклонируемых функций типа арбитр различных конфигураций. Кратко описано построение экспериментальной установки для исследования. Показана зависимость характеристик от длин блока симметричных путей АФНФ, а также выбранного арбитра.

Введение

Физически неклонируемые функции (ФНФ) имеют широкое применение в физической криптографии. Реализованные ФНФ на FPGA привлекательны благодаря относительной простоте реализации и небольшим аппаратурным затратам. Для изучения выбраны ФНФ типа арбитр (АФНФ) [1], реализованные на FPGA Artix 7 фирмы Xilinx, входящих в комплектацию плат быстрого прототипирования Digilent Nexys 4 [2]. Принцип, на котором основывается работа АФНФ, заключается в извлечении производственной энтропии при прохождении тестовых импульсов через звенья АФНФ, выражающейся в различных временных задержках для каждого экземпляра АФНФ. Обычно в классической структуре АФНФ выделяют генератор тестовых сигналов (ГТС), блок симметричных путей (БСП), а также арбитр, отвечающий за выработку ответа ФНФ.

I. Подготовка эксперимента и сбор данных

Для проведения эксперимента на языке VHDL было создано проектное описание экспериментальной установки изучения АФНФ с использованием САПР Vivado 2016.4. Проект включает в себя ГТС, устройство управления на основе цифрового конечного автомата (ЦКА), а также аппаратный генератор М-последовательности в виде сдвигового регистра с линейной обратной связью (linear feedback shift register, LFSR). Передача данных между установкой и ПК организована через интерфейс UART (Universal Asynchronous Receiver-Transmitter). Поддержка передачи данных через UART со стороны экспериментальной установки реализована с использованием IP ядер и софт-процессора Microblaze.

Исследование проводилось для АФНФ различных конфигураций: с различным числом звеньев БСП N ($N = 16$, $N = 32$, $N = 64$ и $N = 128$), а также с арбитрами на базе RS-защелки и D-триггера.

Для определения характеристик АФНФ для всех конфигураций было проведено $E = 10$ экспериментов на $M = 10$ устройствах. Каждый эксперимент включал генерацию $C = 10^6$ запросов к ФНФ и сбор такого же количества ответов. Также для вычисления внутрикристальной уникальности было реализовано $D = 16$ идентичных АФНФ на каждом устройстве.

II. Исследование характеристик АФНФ

Одной из ключевых характеристик ФНФ является стабильность, которая определяет стабильность ответа на фиксированный запрос для конкретного экземпляра ФНФ. Особенно актуальна эта характеристика, например, при использовании ФНФ в качестве средства генерации аппаратного идентификатора. Для классических реализаций АФНФ значение характеристики стабильности может быть снижено из-за особенностей выбранного арбитра, а также изменений внешних условий. Формально значение стабильности $S(CH)$ ответа ФНФ R на запрос CH определяется следующим образом (формула 1):

$$S(CH) = 1 - \frac{1}{E}\sum_{e=1}^{E} HD(R_{ref}, R_e), \qquad (1)$$

где E – количество экспериментов; e – индекс эксперимента; HD – расстояние Хемминга; R_{ref} – эталонное значение ответа на заданный запрос, определяемое по мажоритарному принципу; R_e – ответ на заданный запрос.

Стабильность каждой конфигурации АФНФ определялась как среднее арифметическое всех значений стабильности выполненных запросов и представляется формулой (2):

$$\frac{1}{K}\sum_{i=1}^{k} S(CH_i) \qquad (2)$$

где K – количество запросов, i – индекс запроса.

Полученные результаты характеристик стабильности представлены на рисунке 2.

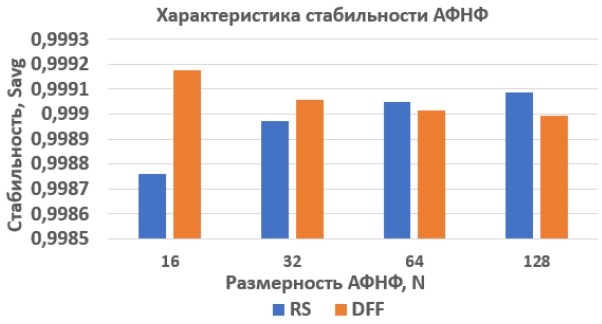

Рис. 1 – Зависимость значения средней стабильности АФНФ от размерности и выбранного арбитра

Метрика уникальности АФНФ для реализаций на идентичных интегральных схемах [3], а также копий АФНФ на одном устройстве, представляет собой усредненное расстояние Хэмминга между экземплярами ФНФ и рассчитывается согласно формуле:

$$U(PUF) = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{l},$$

где m - количество экземпляров ФНФ, l - разрядность ответа ФНФ, бит.

Характеристики внутрикристальной и межкристальной уникальности, полученные в результате эксперимента, представлены на рисунках 2, 3.

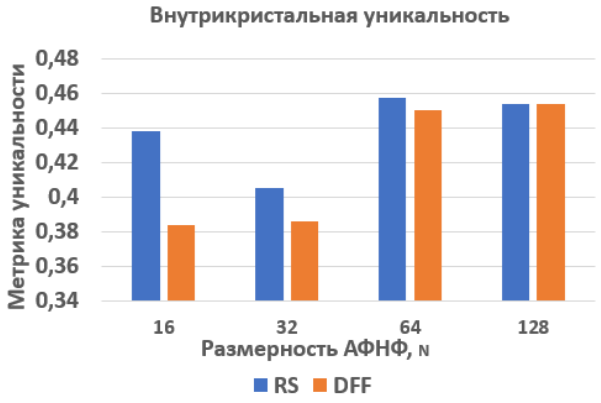

Рис. 2 – Зависимость значения внутрикристальной уникальности АФНФ от размерности и выбранного арбитра

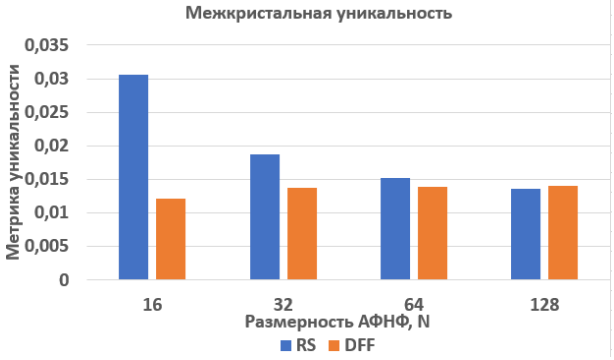

Рис. 3 – Зависимость значения межкристальной уникальности АФНФ от размерности и выбранного арбитра

Для оценки случайности была взята частота появления ответа $r = 1$. Пусть с использованием ФНФ сгенерирована последовательность ответов R длиной n, тогда вероятность появления символа α p_α, встретившегося в R ровно k_α, определяется через отношение:

$$p_\alpha = \frac{k_\alpha}{n}.$$

Экспериментальные результаты p_1 отображены в виде графика на рисунке 4.

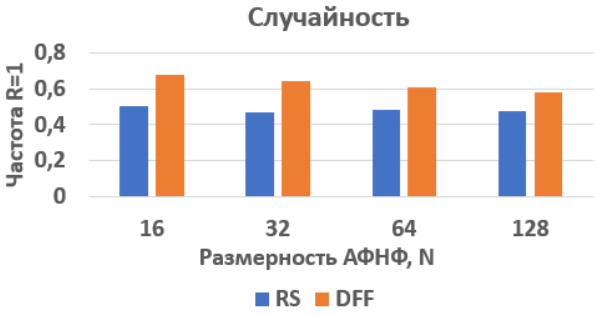

Рис. 4 – Зависимость значения вероятности ответа АФНФ $r = 1$ от размерности и выбранного арбитра

Полученные результаты свидетельствуют о приближении значения p_1 к эталонному $p_1 = 0.5$ при увеличении количества звеньев БСП.

III. Заключение

На основе полученных результатов можно сделать вывод о преимущественно улучшении характеристик ФНФ с увеличением размерности АФНФ. Несколько лучшие характеристики демонстрируют реализации АФНФ с использованием RS-защелки в качестве арбитра. Следует отметить, что при увеличении размерности АФНФ возрастают аппаратурные затраты и время генерации ответа.

Существенным недостатком исследованных реализаций АФНФ являются низкие значения межкристальной уникальности. Это может сильно затруднить их использование и потребовать использования дополнительных модификаций.

IV. Список литературы

1. A technique to build a secret key in integrated circuits for identification and authentication applications / J.W. Lee [et al.] // Intern. Symp. VLSI Circuits (VLSI'04), Honolulu, USA, June 15–19, 2004. – Honolulu, 2004. – P. 176–179
2. Nexys 4 artix-7 FPGA: Trainer board recommended for ece curriculum [Electronic resource]. — Mode of access: https://store.digilentinc.com/nexys-4-artix-7-fpga-trainer-board-limited-time-see-nexys4-ddr/. — Digilent, Inc, 2020. — Date of access: 30.10.2020.
3. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs / Y. Hori [et al.] // Proc. Int. Conf. on Reconfig. Comput. and FPGAs (ReConFig'2010). — Cancun, Mexico, 2010. — P. 298–303.