ПАРАМЕТРИЧЕСКОЕ МОДЕЛИРОВАНИЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Малявко Н.В.

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

Иванюк А.А. – доктор техн. наук, профессор

Улучшена существующая параметрическая модель [1] физически неклонируемой функции типа кольцевой осциллятор путём добавления параметров для моделирования физически неклонируемых функций на технологии программируемых логических интегральных схем. Проведён анализ и сравнение собранных экпериментальных данных с параметрической моделью.

Физически неклонируемая функция (ФНФ) является структурой, позволяющей отображать множество запросов *CH* во множество ответов *R* уникальным и невоспроизводимым образом *CH→R*. В основном ФНФ применяется для генерация случайных чисел и идентификации полупроводниковых устройств. ФНФ представляет собой цифровую схему, создание которой с заранее известными характеристиками практически невозможно. Существует множество схем цифровых ФНФ, большинство из которых основаны на уникальности задержек распространения сигналов. К таким схемам относятся ФНФ типа арбитр [2] и кольцевой осциллятор (КО) [3].

Симметрия является определяющим фактором работоспособности схем ФНФ. Если симметрию можно достичь при проектировании и изготовлении специализированных интегральных схем, то для программируемых логических интегральных схем это практически невозможно. Два пути являются симметричными, если задержка распространения сигнала по одному пути равна задержке распространения сигнала по второму пути. Можно выделить следующие виды симметрии путей: структурную, топологическую и физическую. Структурную симметрию путей можно достичь на стадии проектирования цифрового устройства путём расположения одинаковых функциональных элементов. Топологическая симметрия может быть обеспечена идентичным расположением копий элементов двух путей и их межсоединений. Наибольшая физическая симметрия может быть обеспечена при изготовлении полупроводникового кристалла. При этом физическая симметрия бывает двух типов: внутрикристальная и межкристальная. Если идеальную проектную и топологическую симметрию можно обеспечить на практике, то идеальная физическая симметрия недостижима по многим причинам. В первую очередь связанным с девиациями материалов и технологических операций при изготовлении полупроводниковых кристаллов. Это выражается в разности задержек распространения сигналов по симметричным путям, а возможность измерения и сравнения такой разности лежит в основе построения цифровых ФНФ.

В расширенной программной модели ФНФ КО задержка сигнала определяется как:

$$\Delta = \delta_b + \delta_t + \delta_d, \tag{1}$$

где δ_b – задержка распространения сигнала через кольцевой осциллятор; δ_t – задержка распространения сигнала через межсоединения; δ_d – зависящая от условий эксплуатации случайная задержка, которая различна при каждом измерении. Схема вычисления пары *CH→R* представлена на рисунке 1.

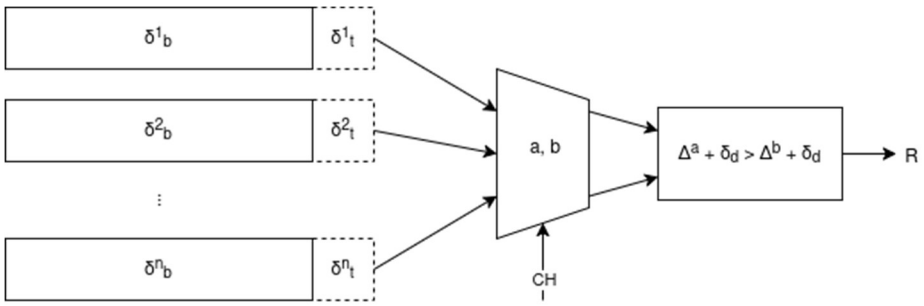
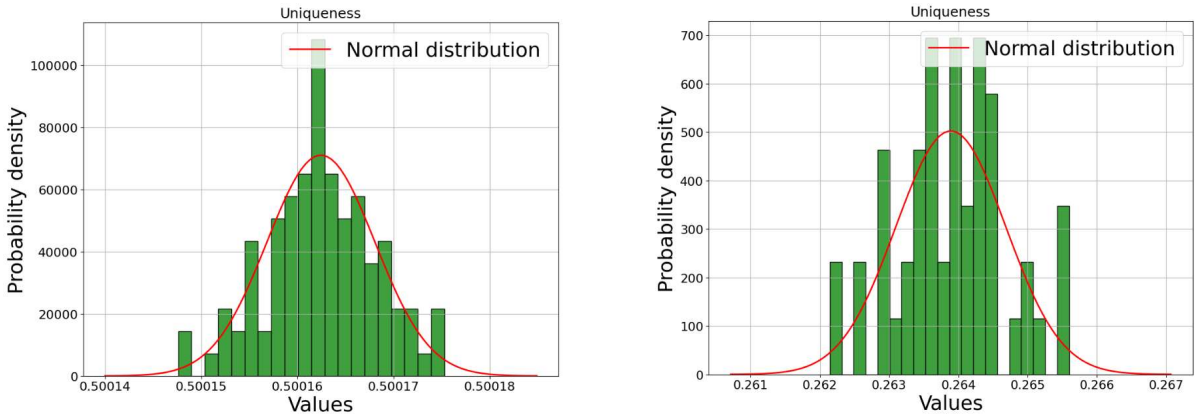


Рисунок 1 – Модель ФНФ типа КО, реализованная программно. Обозначения для задержек взяты из формулы (1). Δ^a и Δ^b – задержки под индексом a, b.

Был проанализирован собранный для работы [4] набор данных с кластера ПЛИС. Кластер состоял из четырех Xilinx ZYNQ 7000. На каждой ПЛИС было размещено четыре ФНФ КО с фиксированным размещением. Фиксированное размещение означает, что на этапе задания проектного

описания указывалось конкретное размещение LUT-блоков, а межсоединения закреплялись путем описания их подключений к конкретным физическим входам. Размещение одной схемы дублировалось на идентичных смежных блоках ПЛИС для обеспечения максимального подобия четырёх экземпляров ФНФ КО.

Набор данных представлял частоты для каждого КО в структуре ФНФ. Для определения корректности параметрической модели выделим такие метрики как, единообразие, стабильность, надёжность и уникальность. Объяснения физического смысла метрик и формулы их расчёта показаны в работе [5]. Особое внимание уделим метрикам внутрикристальной уникальности и единообразия. Для сравнения программной модели с экспериментом возьмём результаты из таблицы 4 в работе [4]. Исходя из таблицы, значение метрики внутрикристальной уникальности лежит в диапазоне [0,34; 0.48] для стратегии автоматического размещения и [0,07; 0,12] для стратегии фиксированного размещения. Модель показала центры распределения метрики внутрикристальной уникальности в точках 0,500 для моделирования автоматического размещения ФНФ на ПЛИС и 0,264 *для моделирования фиксированного размещения ФНФ на ПЛИС, что эквивалентно моделированию размещения ФНФ на интегральной схеме специального назначения.* Распределения метрик внутрикристальной уникальности при моделировании представлены на рисунке 2. Центр распределения метрик единообразия при моделировании попал в диапазон [0,985; 0,995], что согласуется с результатами из таблицы 3 в работе [4].



а) б)

Рисунок 2 – распределение метрики внутрикристальной уникальности для моделирования ФНФ КО на ПЛИС (а). Распределение метрики внутрикристальной уникальности для моделирования ФНФ КО на специализированной интегральной схеме (б).

Можно сделать вывод, что определяющим результат моделирования фактором является сотношение величин задержек. Например, задержки δ_b и δ_t для двух КО будут близки, значит определяющим результат будет значение δ_d, которое принимает случайное значение при каждом измерении. В таком случае ФНФ хорошо применима для задачи генерации случайных чисел. В ином случае, где задержка δ_b или δ_t много больше остальных, ФНФ решает задачу идентификации, ведь тогда появляются стабильные пары *CH→R*. Результаты, полученные при параметрическом моделировании ФНФ КО похожи по природе с экспериментальными данными. Из этого можно сделать вывод о состоятельности программной модели и применимости её для моделирования ФНФ типа КО.

Список использованных источников:

1. Малявко Н.В., Иванюк А.А. Алгоритмы параметрического моделирования физически неклонируемых функций. Информационные технологии и системы 2024, 91-92. https://its.bsuir.by/m/12_130111_1_190875.pdf

2. S. Hemavathy and V. S. K. Bhaaskaran, "Arbiter PUF—A Review of Design, Composition, and Security Aspects," in IEEE Access, vol. 11, pp. 33979-34004, 2023, doi: 10.1109/ACCESS.2023.3264016.

3. G. Edward Suh and Srinivas Devadas. 2007. Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th annual Design Automation Conference (DAC '07). Association for Computing Machinery, New York, NY, USA, 9–14. https://doi.org/10.1145/1278480.1278484

4. Иванюк А.А. Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора. Информатика. 2025;22(1):73-89. https://doi.org/10.37661/1816-0301-2025-22-1-73-89

5. Martin H, Peris-Lopez P, Natale GD, Taouil M, Hamdioui S. Enhancing PUF Based Challenge–Response Sets by Exploiting Various Background Noise Configurations. Electronics. 2019; 8(2):145. https://doi.org/10.3390/electronics8020145