АЛГОРИТМЫ ПАРАМЕТРИЧЕСКОГО МОДЕЛИРОВАНИЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ

Малявко Н. В., Иванюк А. А.
Факультет компьютерных систем и сетей, кафедра программного обеспечения информационных технологий,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: mikita.maliauka@gmail.com, ivaniuk@bsuir.by

В работе построена программная модель для параметрического моделирования физически неклонируемой функций типа кольцевой осцилятор. Проведено программное моделирование и рассчитана метрика единообразия.

Введение

В настоящее время актуальным является использование физической криптографии, основанной на невоспроизводимости некоторых параметров и характеристик физических систем. В области физической криптографии распространено использование физически неклонируемых функций (ФНФ)[1-3].

ФНФ является структурой, позволяющей отображать множество запросов CH во множество ответов R уникальным и невоспроизводимым образом $CH \rightarrow R$. В цифровых устройствах преобладает использование ФНФ, базирующихся на уникальности и невоспроизводимости задержек распространения сигналов через их пути. Одним из таких типов ФНФ является ФНФ типа кольцевой осцилятор (КО).

Эта ФНФ выдаёт однобитный ответ путём сравнения частот двух КО.

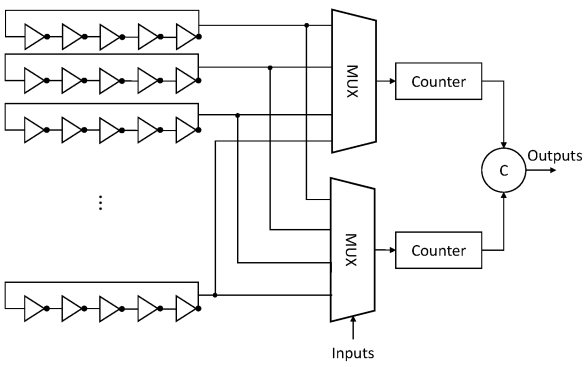

Рис. 1 – ФНФ типа кольцевой осцилятор

КО – цифровой генератор, состоящий из нечётного числа инверторов соединённых последовательно и замкнутых петлёй обратной связи, который колеблется на определённой частоте. Частота колебаний КО определяется особенностью реализации (количество инверторов или других элементов задержки, маршрутов на кристалле), случайными технологическими отклонениями и условиями эксплуатации, которые оказывают уникальное влияние на каждое устройство.

Традиционная схема ФНФ типа КО представлена на рисунке 1. Она измеряет частоты пары КО (f_i,f_j) с помощью двух счётчиков и сравнивает эти две частоты, чтобы сформировать бит ответа r_{ij} на основе следующего правила:

$$r_{ij} = \begin{cases} 1 \text{ если } f_i > f_j \\ 0 \text{ иначе} \end{cases} .$$

N-битная сигнатура может быть создана путём сравнения нескольких КО. Обычно эти КО реализуются в двумерной матрице [1].

I. Описание параметрической модели

Значение задержки на КО будет рассчитываться по следующей формуле:

$$delay = \sum_{i=1}^{n} pd_i,$$

где pd_i – задержка на каждом инверторе.

В программной модели было сделано допущение, что задержка КО генерируется как нормально распределённое случайное число в определённом диапазоне значений.

Из-за особенностей технологии производства невозможно гарантировать, что задержка на элементе будет иметь точное значение. Оно будет отличаться на случайную величину, назовём её дивиацией, от среднего значения задержки для конкретного технологического процесса[4]. Тогда суммарная задержка на КО будет рассчитываться как:

$$delay = \sum_{i=1}^{n} pd_i \times (1 + diviation_i),$$

где pd_i – задержка на каждом инверторе и $diviation_i$ – процент отклонения от среднего значения.

В аппаратуре выбор случайных пар КО реализовывается через мультиплексоры и другой КО, который непосредственно выбирает пару. В программной модели ФНФ выбиралась пара КО при помощи стандартной функции генерации случайных чисел.

Работа выполнена в совместной учебной лаборатории БГУИР-YADRO
`https://www.bsuir.by/ru/kaf-informatiki/yadro`

II. Исследование параметрической модели

Двоичная ФНФ является единообразной, если в n-битовом ответе содержится равное количество нулей и едениц [3]. Единообразие можно рассчитать следующим образом:

$$uniformity = \frac{1}{n}\sum_{l=1}^{n} r_l,$$

где r_l представляет собой l-бит n-битного отклика. После вычисления метрики единообразия со случайными и одинаковыми задержками на 10000 прогонах, центр распределения оказался в: $uniformity_{diff} = 0.499542$ (рисунок 2) и $uniformity_{same} = 0.499569$ (рисунок 3). Эти значения единообразия отличаются на $\simeq 0.06\%$ от значения полученным авторами в работе [3].

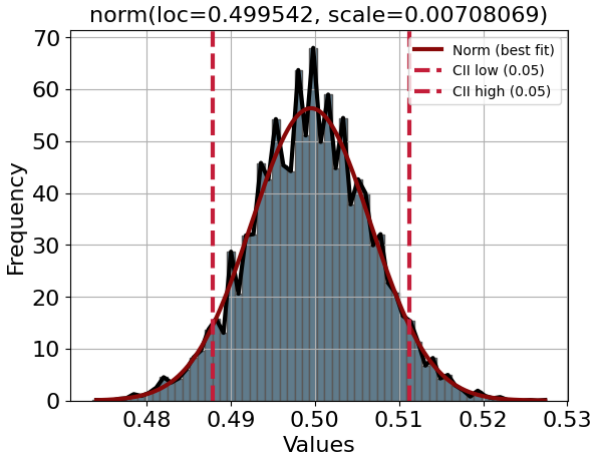

Рис. 2 – Распределение единообразия для 10000 прогонов модели со случайными задержками

Из полученных данных мы можем сделать вывод, что на метрику единообразие не влияет количество инверторов в КО. И что важно наличие девиации в модели. Это знание может быть использовано для экономии аппаратных ресурсов: энергопотребления и места на кристалле.

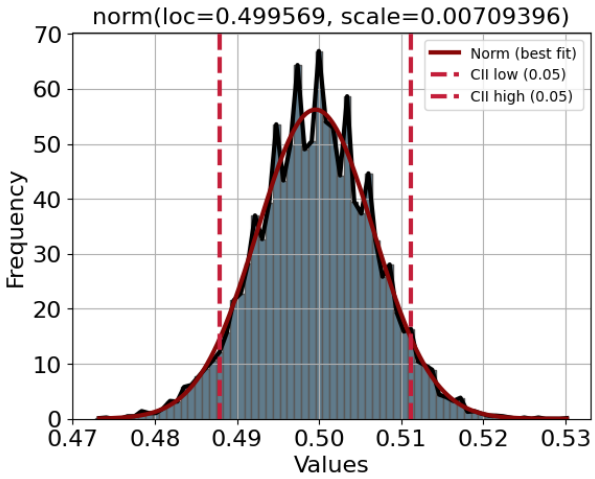

Рис. 3 – Распределение единообразия для 10000 прогонов модели с одинаковыми задержками и девиацией

III. Заключение

Результатом работы является программная модель, которая описывает ФНФ типа КО и совпадает по рассматриваемым метрикам с метриками, полученными на основе собранных с реальной аппаратуры данных[3]. А так же учитывает следующий набор параметров:

- количество КО;
- флаг генерации одинаковых задержек;
- размернотсь битового вектора ответов;
- диапазон значений задержки распространения сигнала;
- диапазон значений девиации.

Модель может быть расширена путём добавления новых параметров для анализа свойств ФНФ типа КО.

IV. Список литературы

1. D. Lim, Extracting Secret Keys from Integrated Circuits, Master's Thesis, MIT, 2004.
2. 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
3. G. Edward Suh, 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. Шамына, А. Ю. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора=Investigation of the Timing Parameters of The Arbiter-Based Physically Unclonable Function Using a Ring Oscillator / Шамына А. Ю., Иванюк А. А. // Цифровая трансформация. – 2022. – Т. 28, № 1. – С. 27–38. DOI: http://doi.org/10.35596/2522-9613-2022-28-1-27-38.