ИСПОЛЬЗОВАНИЕ АСИНХРОННЫХ D-ТРИГГЕРОВ ДЛЯ ГЕНЕРАЦИИ УНИКАЛЬНЫХ ЦИФРОВЫХ ИДЕНТИФИКАТОРОВ

Кохновский С.И.

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

Иванюк А.А. – д.т.н., профессор

В работе представлены результаты эксперимента с использованием асинхронных D-триггеров в качестве устройств генерации цифровых идентификаторов на этапе инициализации ПЛИС.

Достаточно давно была предложена идея использования случайных внутренних физических особенностей цифровых устройств в качестве средств их идентификации. Эта идея была воплощена в физически неклонируемых функциях (ФНФ). Среди множества различных вариантов реализации особый интерес вызывают расположенные на кристалле ФНФ, что само по себе является значительным преимуществом из-за возможности прямого использования запускаемыми на этом же кристалле приложениями. Одним из первых вариантов реализации стали ФНФ, основанные на принципах работы кольцевых осцилляторов (RO-PUFs) [1].

В качестве источника энтропии выбрана схема на основе D-триггера с кольцевым осциллятором (ROLD), детально описанная в работе [2]. Реализация источника случайности была произведена на плате быстрого прототипирования Digilent Nexys 4 в САПР Xilinx Vivado 2020.2 с использованием элементов комбинационной логики – LUT-блоков. Для проведения эксперимента использованы 8 IP-компонент, содержащих по 32 вышеописанных источника энтропии. С целью получения данных из компонент использован процессор MicroBlaze на рабочей частоте 100 MHz.

На этапе инициализации схема ведёт себя подобно функционированию ФНФ типа SRAM, которые используют в качестве источника случайности колебания свойств транзисторов, возникающих на этапе производства, на микросхеме [3]. Для демонстрации данного поведения вычислено значение вероятности $P_i = \frac{1}{1000}\sum_{e=1}^{1000} Q_i^e, Q_i^e \in \{0,1\}$ генерации единичного символа $Q_i = '1', i \in [0; 255]$ на 1000 экспериментах источником случайности (рисунок 1).

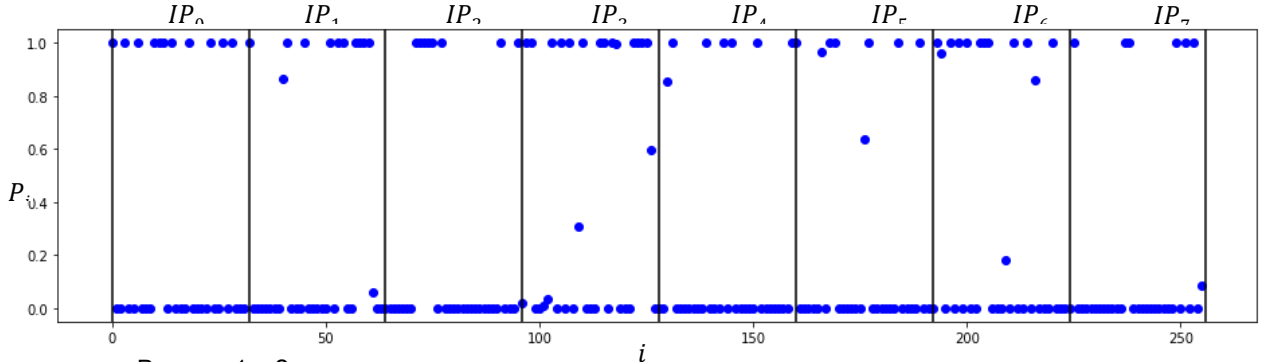

Рисунок 1 – Значения вероятности генераций единичного символа источниками энтропии

В результате эксперимента на этапе инициализации стабильное нулевое значение $P_i = 0$ приняли 170 генераторов, в стабильном единичном значении $P_i = 1$ пребывали 70 источников случайности, а 16 находились в метастабильном состоянии $0 < P_i < 1$.

Данный результат показывает наличие у асинхронных D-триггеров свойств ФНФ типа SRAM, что делает возможным их использование для генерации случайных уникальных идентификаторов. Одним из возможных вариантов использования уникального идентификатора является их применение в качестве начального значения для генерации последовательностей случайных чисел.

Список использованных источников:

1. Gassend, B., Clarke, D., van Dijk, M., Devadas, S.: Silicon physical random functions. In: ACM Conference on Computer and Communications Security, pp. 148–160. ACM Press, New York, NY, USA (2002)

2. Кохновский, С. И., Иванюк А. А. Влияние длительности работы кольцевого осциллятора на статистические характеристики последовательности бит, сгенерированной аппаратным генератором случайных чисел [Электронный ресурс] / С. И. Кохновский, А. А. Иванюк // Информационные технологии и системы 2021 (ИТС 2021) : материалы междунар. науч. конф. – Минск : БГУИР, 2021. – 248 с. – С. 126-127. – Режим доступа: https://its.bsuir.by/m/12_130111_1_157684.pdf. – Дата доступа: 08.04.2022.

3. Holcomb, D.E., Burleson, W.P., Fu, K.: Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In: Proceedings of the Conference on RFID Security (2007)