ИССЛЕДОВАНИЕ ПАРАМЕТРОВ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА СОЗУ НА ПЛИС

Дранкевич А.А.

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

Иванюк А.А. – д.т.н., проф.

В работе оцениваются основные характеристики ФНФ типа СОЗУ, реализованной на Xilinx XC7A100T-1CSG324C, входящей в состав платы быстрого прототипирования Xilinx Digilent Nexys 4.

В настоящее время все большая роль и значение отводятся средствам физической криптографии. Одним из наиболее популярных направлений является изучение физически неклонируемых функций (ФНФ) [1]. ФНФ – это физические системы (устройства), неотъемлемым свойством которых является неклонируемость (неповторяемость) некоторых их функций, свойств, характеристик либо параметров [2]. ФНФ состоят из множества компонент, параметры которых при создании принимают случайные значения, которыми, ввиду их сущности, невозможно управлять. Существует разные типы ФНФ в компьютерной цифровой технике, такие как арбитр, статическое оперативное запоминающее устройство (СОЗУ), кольцевой генератор и др. [3].

Цель данной работы - воспроизвести ФНФ типа СОЗУ на плате быстрого прототипирования Xilinx Nexys 4 для изучения стабильности, единообразия и уникальности полученных значений [4]. В работе ФНФ реализовалась как бистабильный элемент, состоящий из двух последовательно соединенных инверторов. Бистабильный элемент, так же однобитная ячейка памяти, может хранить одно из состояний, логический 0 или 1 [5]. При включении питания состояние элемента зависит от многих параметров, однако в конечном итоге элемент перейдет в одно из своих стабильных состояний, значение которого считается случайным. По своей природе, любое малейшее колебание выведет элемент из метастабильного состояния в одно из стабильных, но не наоборот. Реализация на ПЛИС бистабильного элемента представляет собой две аппаратные таблицы истинности (LUT), соединенные между собой. Аппаратная таблица истинности может реализовать собой любую логическую функцию, заданую таблицей истинности, ограничиваясь только количеством ее аргументов и значений [6]. ПЛИС FPGA Xilinx Nexys 4 располагает ресурсом 63400 аппаратных таблиц истинности, принимающих 6 аргументов и позволяющих получить одно выходное значение (LUT6) [7]. Для сбора последовательностей и последующего их анализа на ПЛИС был использован soft-processor Microblaze с дополнительными аппаратными блоками, обеспечивающих связь и управление реализованной ФНФ. Остальная часть ПЛИС была заполнена бистабильными элементами, суммарная размерность получаемой последовательности составила 25088 бит. Утилизация возможностей ПЛИС для генерации последовательности составила 79,1%. Эксперименты по генерации случайных последовательностей происходили по следующей схеме:

1. ПЛИС подключается к управляющему устройству (ПК).
2. ПЛИС реконфигурируется, тем самым на бистабильных элементах фиксируются полученные значения битов.
3. Управляющие блоки Microblaze собирают значиения бистабильных элементов в бинарную последовательность.
4. ПК загружает бинарную последовательность с ПЛИС.
5. Пункты 2-4 повторяются *N* раз для *K* ПЛИС.

Таким образом, при *N* = 100 и *K* = 10 были получены бинарные последовательности суммарной длиной 3 Мб для дальнейшего анализа. Получив *N* последовательностей на каждой ПЛИС, были подсчитаны математические ожидания каждого бита μ_i. Распределение μ_i показано на рисунке 1а. На их основе, были получены следующие значения: вероятность стабильного нуля p_0 = 0.4676 ± 0.83%, вероятность стабильной единицы p_1 = 0.5324 ± 0.73%, вероятность нестабильного значения p_X = 0.0916 ± 11.93%, их сумма равна 1. Вариация здесь и далее указана между ПЛИС.

Единообразие *U* для ПЛИС вычисляется по формуле:

$$U = 1 - 2 * \left| \frac{p_1}{p_0 + p_1} - \mu_t \right|, \quad (1)$$

где μ_t – математическое ожидание идеального бистабильного элемента, μ_t = 0,5000.

Полученное значение среди ПЛИС *U* = 0,9300 ± 0,87%, что объясняется особенностью технологического расположения бистабильных элементов на ПЛИС. Распределение единообразия представлено на рисунке 1б.

Стабильность *S* для ФНФ – относительное количество нестабильных элементов. Для всех ПЛИС, полученное значение стабильности *S* = 0.9084 ± 1.2%. Полученная стабильность высокая, что

объясняется особенностью технологического расположения бистабильных элементов на ПЛИС и соединения отдельных ее компонентов.

Для вычисления уникальности нестабильные значения битов округлялись до соответствующих им стабильных значений.

Внутрикристальная уникальность последовательностей проверялась с помощью вычисления расстояний по Хэммингу между отдельными словами последовательности. Ожидаемое распределение биномиальное с параметром $p = \mu_t$. Соответствие этому распределению означает равномерное распределение случайных битов, и, соответственно, их независимость от расположения на ПЛИС. Полученное распределение практически не зависит от ПЛИС, так как среднее отклонение мало.

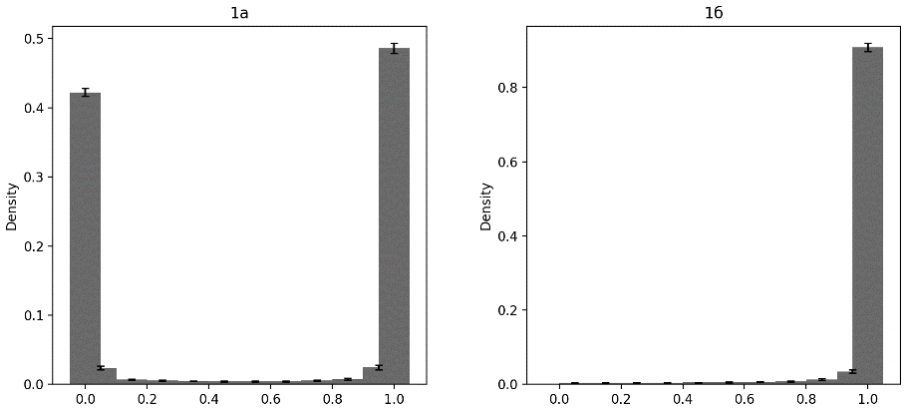

Рисунок 1а – Распределение μ_i; 1б – Распределение единообразия

Уникальность последовательностей между запусками на одной и той же ПЛИС проверялась путем вычисления расстояний по Хэммингу между полученными последовательностями. Уникальность можно предсказать из распределения стабильностей. Проинтегрировав их, априорная уникальность составила 0,0193 ± 13,29%, апостериорная 0,0195 ± 13,29%. Вариация результатов между ПЛИС велика, это объясняется большим различием в их внутренней структуре. Небольшое значение объясняется малым количеством нестабильных битов.

Межкристальная уникальность последовательностей между ПЛИС проверялась путем вычисления расстояний по Хэммингу между полученными стабильностями. Полученная уникальность составила 0,2444 ± 0%, что объясняется большой вариацией относительных расстояний между ПЛИС. То есть, количество битов, которые будут различны в последовательности, больше примерно в 12,5 раз между ПЛИС, чем на одной. Несмотря на это, большинство из этих отличных битов будут стабильными.

Бистабильный элемент считается слабой ФНФ, то есть напрямую полученные значения нельзя применять как равномерное случайное число, более того, размер такой последовательности сильно ограничен. В дальнейшем результаты данного исследования планируется использовать для создания сильной ФНФ и применимости последовательностей для генерации равномерно распределенных случайных чисел во время работы ПЛИС.

Список использованных источников:

1. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu. – Cambridge : Massachusetts Institute of Technology, 2001. – 154 p.

2. Tuyls P. Security with Noisy Data // Springer : London, 2007. – 344 p.

3. Lata, K.; Cenkeramaddi, L.R. FPGA-Based PUF Designs: A Comprehensive Review and Comparative Analysis. // Cryptography 2023, 7, 55. – Режим доступа: https://doi.org/10.3390/cryptography7040055. 7–14 p.

4. Athanas P., Pnevmatikatos D., Sklavos N. (eds.) (2013) A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions. Embedded Systems Design with FPGAs. New York, Springer. 245–267 p.

5. B. HOLDSWORTH BSc (Eng), MSc, FIEE, R.C. WOODS MA, DPhil, in Digital Logic Design (Fourth Edition), 2002. 142–144 p.

6. HardwareBee [Электронный ресурс]. – Overview of Lookup Tables (LUT) in FPGA Design. – Режим доступа: https://hardwarebee.com/overview-of-lookup-tables-in-fpga-design/. – Дата доступа: 25.03.2023.

7. Diligent Reference [Электронный ресурс]. – Nexys 4. – Режим доступа: https://digilent.com/reference/programmable-logic/nexys-4/start. – Дата доступа: 25.03.2023.