http://doi.org/10.35596/2522-9613-2022-28-1-27-38

Оригинальная статья
Original paper

УДК 681.324

ИССЛЕДОВАНИЕ ВРЕМЕННЫХ ПАРАМЕТРОВ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА АРБИТР С ИСПОЛЬЗОВАНИЕМ КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

А.Ю. ШАМЫНА, А.А. ИВАНЮК

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

Поступила в редакцию 26 сентября 2021

Аннотация. Рассматривается возможность использования схемы кольцевого осциллятора для измерения задержек распространения сигналов через симметричные пути различных длин, реализованных на FPGA. Описывается создание экспериментальной установки и ход проведения экспериментов. Исследуется зависимость абсолютных значений задержек распространения сигналов и их статистических характеристик от количества блоков симметричных путей. Рассчитываются метрики стабильности и межкристальной уникальности на основе полученных экспериментальных данных измерений задержек. Подтверждается улучшение характеристик стабильности и уникальности значений задержек с увеличением длины симметричных путей АФНФ.

Ключевые слова: физическая криптография, физически неклонируемые функции, кольцевой осциллятор, физически неклонируемая функция типа арбитр.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Шамына А.Ю., Иванюк А.А. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора. Цифровая трансформация. 2022; 28(1): 27-38.

INVESTIGATION OF THE TIMING PARAMETERS OF THE ARBITER-BASED PHYSICALLY UNCLONABLE FUNCTION USING A RING OSCILLATOR

ARTSIOM YU. SHAMYNA, ALEXANDER A. IVANIUK

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Submitted 26 September 2021

Abstract. The possibility of using a ring oscillator circuit for measuring the propagation delays of signals through symmetrical APUF paths of various lengths implemented on an FPGA is considered. The creation of the experimental setup and the course of the experiments are described. The dependence of the absolute values of the signal propagation delays and their statistical characteristics on the number of blocks of the symmetric paths under study is investigated. The metrics of stability and intercrystalline uniqueness are calculated based on the obtained experimental data of delay measurements. The improvement of APUF stability and uniqueness depending on the length of the symmetric paths is confirmed.

Keywords: physical cryptography, physically unclonable functions, ring oscillator, arbiter-based physically unclonable function.

Conflict of interests. The authors declare no conflict of interests.

For citation. Shamyna A.Yu, Ivaniuk A.A. Investigation of the Timing Parameters of The Arbiter-Based Physically Unclonable Function Using a Ring Oscillator. Digital transformation. 2022; 28(1): 27-38.

Введение

Оценка задержек распространения сигналов по путям цифровых устройств имеет важное значение при их проектировании. От этого напрямую зависит надежность устройств и стабильность их характеристик в заданных режимах работы. Однако следует отметить невозможность создания нескольких устройств с идентичными характеристиками, в том числе и характеристикой распространения сигналов через одинаковые по своей функциональности и топологии составные части [1–3]. Это обусловлено несовершенством производственного процесса, а также физическими вариациями материалов, используемых при их производстве. Данный факт осложняет процесс массового тиражирования устройств, поэтому на практике часто используют консервативные модельные оценки задержек, которые на основе усредненных значений и некоторых допущений позволяют получить значение задержки по некоторому пути цифрового устройства, а также пренебречь их естественными флуктуациями при производстве конкретных экземпляров. Следует отметить, что у уникальности задержек по фиксированным путям от устройства к устройству есть практическое применение. Например, это явление лежит в основе функционирования многих видов физически неклонируемых функций (ФНФ) [4]. На этом принципе строятся такие виды ФНФ как ФНФ типа арбитр, ФНФ на базе кольцевых осцилляторов, комбинированные ФНФ и др. [5–10]. Однако при реализации цифровых схем с использованием современных технологий прямые измерения задержек осложнены, а использование методов оценок разниц задержек, например, на основе D-триггера, как в случае ФНФ типа арбитр, позволяет оценить лишь временную разницу фиксации фронтов тестового импульса и не позволяет перейти к абсолютным значениям. Более того, в таком случае проявляется негативный эффект метастабильности D-триггера, который возникает при нарушении условий удержания и предустановки входных сигналов. Данное явление может снизить достоверность оценки задержек для выбранного пути цифрового устройства.

По мнению авторов, более подходящим для детального исследования задержек распространения сигналов по фиксированному пути является подход, основанный на принципе работы кольцевого осциллятора (КО) и охвате исследуемого пути Path отрицательной обратной связью, когда частота формируемой им импульсной последовательности зависит от суммарных задержек элементов, входящих в ее состав. Кроме этого, при измерении частоты импульсов, формируемых КО, счетчиком Counter можно пренебречь величиной задержки соединительного проводника от выхода КО до входа счетчика, чего сложно добиться при использовании других схем оценки задержек. В цепь обратной связи добавлен двухвходовой элемент 2И-НЕ для обеспечения возможности управления режимом КО схемы, а также обеспечения инверсии проходящего через нее сигнала. Для управления окном измерения и выработки сигнала разрешения функционирования кольцевого генератора START используется компонент Control unit. При подаче высокого уровня сигнала START схема переходит в режим осцилляции и формирует импульсную последовательность на выходе RO_OUT, которая подается на синхронный вход счетчика Counter. После эксперимента данные измерения снимаются

с выходной шины D_OUT счетчика Counter. Обобщенно рассматриваемое решение схематично представлено на рис. 1.

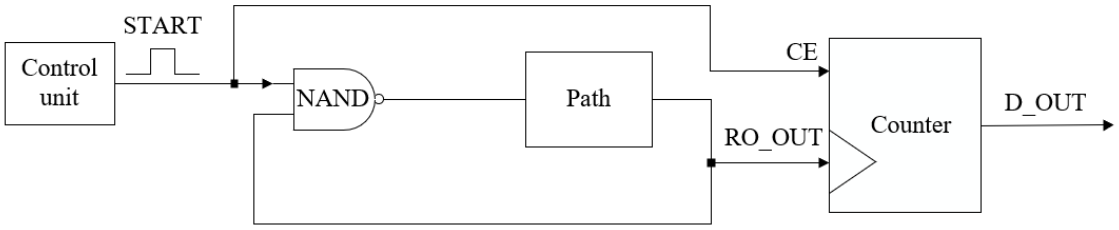

Рис. 1. Схема измерения задержек распространения сигналов на основе КО
Fig. 1. Circuit scheme for measuring signal propagation delays based on Ring Oscillator

В настоящей работе исследуются задержки распространения сигналов по двум симметричным путям ФНФ типа арбитр (АФНФ) с использованием подхода на базе КО, описанного выше. Анализируется зависимость характеристик задержек от количества базовых элементов в исследуемом пути цифрового устройства.

Построение экспериментальной установки для исследования

В данной работе исследуются задержки распространения сигналов по двум симметричным путям АФНФ с использованием подхода на базе КО [9]. Для этого была изменена классическая схема блока симметричных путей АФНФ, которая представляет собой два конфигурируемых пути. В частности, выходы последнего блока были соединены через элементы И-НЕ со входами первого блока для создания цепей обратной связи КО, а также возможности управления ими. Конфигурация путей осуществляется подачей на схему n-разрядного вектора запроса $C_i = c_0\, c_1\, c_2 \ldots\, c_{n-1}$, где $c_j \in \{0,1\}$, $j \in \{0, 1, 2, \ldots, n-1\}$. Уникальность конфигураций путей для каждого C_i запроса достигается благодаря прямой передаче сигнала через звено симметричных путей $Link_j$ при $c_j = 0$ и перекрестной при $c_j = 1$ соответственно. Включение режима осциллятора для схемы происходит путем подачи высокого уровня сигнала *Start*, который удерживается фиксированное время D_s для каждого запроса. Для измерений формируемых частот двух полученных КО используются два синхронных 32-разрядных счетчика *Counter*, которые работают то же фиксированное время D_s, что и удерживается режим работы КО для исследуемой схемы (рис. 2).

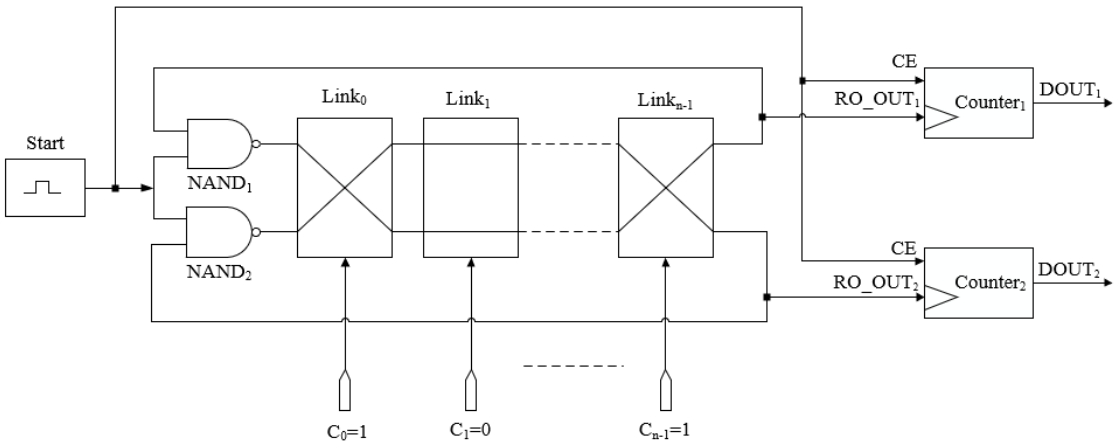

Рис. 2. Схема измерения задержек распространения сигналов через симметричные пути на основе КО
Fig. 2. Circuit scheme for measuring signal propagation delays through symmetric paths based on Ring Oscillator

Однако схема, представленная на рис. 2, имеет недостаток, который осложняет измерения задержек путей АФНФ. Предположим, что при некотором запросе будет нечетное количество блоков с перекрестной передачей сигналов. Тогда выход элемента $NAND_1$ будет соединен со входом элемента $NAND_2$ и наоборот, что значительно удлиняет охватываемый обратной связью путь, а также делает невозможным функционирование КО из-за четного количества инверторов в схеме. Таким образом, в случае соответствия перекрестной передаче тестовых сигналов через звено $Link_j$ значению запроса $C_j = 1$ при нечетном количестве таких разрядов в запросе предложенная схема не позволяет измерять задержки.

Для измерения задержек путей схемы, соответствующим любым запросам, а не только с четным количеством $C_j = 1$, описанная выше схема была модифицирована добавлением в блок симметричных путей корректирующего звена $Link_n$. Значение управляющего сигнала для этого блока определяется не разрядом запроса, а результатом операции суммы по модулю 2 всех значений разрядов текущего запроса. Такой подход позволяет обеспечить работу двух независимых КО в исследуемой схеме при любом значении запроса. Вносимые дополнительным блоком задержки принципиально не изменяют вычисляемых характеристик суммарных задержек. Модифицированная схема представлена на рис. 3.

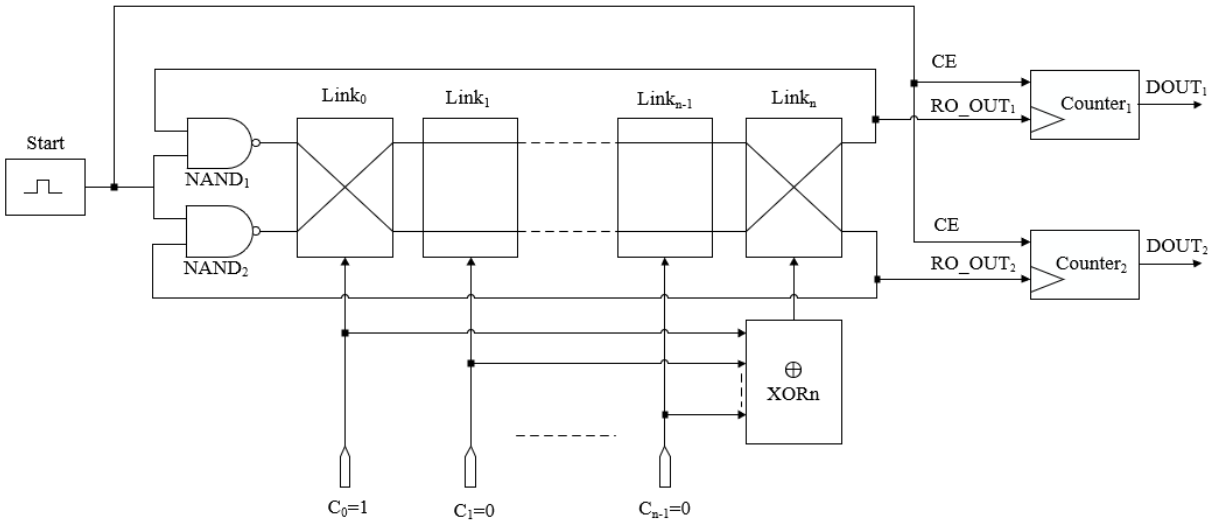

Рис. 3. Модифицированная схема измерения задержек распространения сигналов через симметричные пути на основе КО

Fig. 3. Modified circuit scheme for measuring signal propagation delays through symmetric paths based on Ring Oscillator

Управлением экспериментом осуществлялось с использованием устройства управления *FSM* и софт-процессора *Microblaze*. Устройство управления использовалось для генерации управляющих сигналов подчиненных устройств в соответствии со своим состоянием, устанавливаемым *Microblaze*. Также с его помощью на уровне программного кода осуществлялась генерация запросов, происходило считывание значений регистров счетчиков экспериментальной установки, а также выполнялась передача данных на ПК. Кроме самостоятельно созданных VHDL-модулей были использованы стандартные IP-ядра для обеспечения поддержки передачи данных через UART-интерфейс и взаимодействия софт-процессора с другими компонентами через GPIO (рис. 4).

Проектное описание экспериментальной установки было создано на языке VHDL в САПР Vivado 2018.2. Написание программного кода для Microblaze, а также его отладка выполнялась средствами Xilinx SDK. Конфигурация всех FPGA выполнялась с использованием одного битового образа, сгенерированного Vivado 2018.2. Программирование FPGA осуществлялось с использованием Hardware Manager среды Vivado 2018.2.

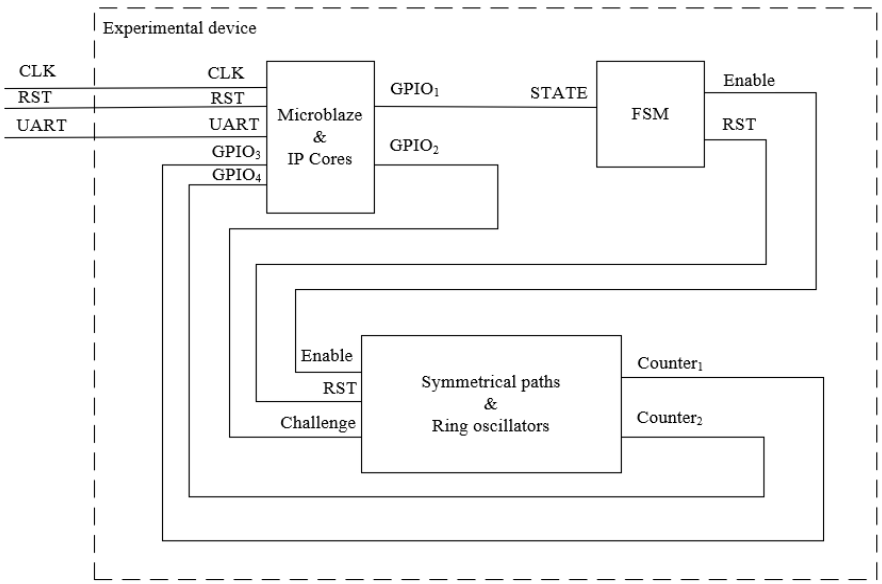

Рис. 4. Экспериментальное устройство
Fig. 4. Experimental device

Основной целью работы являлось исследование зависимости характеристик задержек распространения сигналов через симметричные пути АФНФ от количества элементов, поэтому серия экспериментов была проведена для нескольких конфигураций симметричных путей с различным количеством N звеньев, где $N \in \{8–20, 32, 64, 128\}$. Для конфигураций с длинами $N \in [8;20]$ были поданы все 2^N запросов. Генерация запросов для длин путей $N \in \{32, 64, 128\}$ осуществлялась с использованием генератора псевдослучайной последовательности на основе сдвигового регистра с линейной обратной связью (LFSR). Для каждой конфигурации было проведено $C = 10^6$ измерений. Все эксперименты были повторены $E = 10$ раз. Эксперименты проводились на $M = 5$ платах быстрого прототипирования Digilent Nexys 4 с FPGA Xilinx Artix 7 (xc7a100tcsg324-1), изготовленных по технологическому процессу 45 нм. Для одновременной работы с несколькими платами использовался USB-хаб с активным питанием Sipolar A-423. Схема экспериментальной установки представлена на рис. 5.

Создание проектного описания, управление ходом проведения экспериментов и запись их результатов выполнялись на персональном компьютере *Host PC*. Запись в текстовые файлы экспериментальных данных с COM-портов осуществлялась с использованием ПО Tera Term. Для дальнейшей обработки экспериментальных данных и расчета полученных значений было создано консольное приложение на языке C# в IDE Visual Studio 2019.

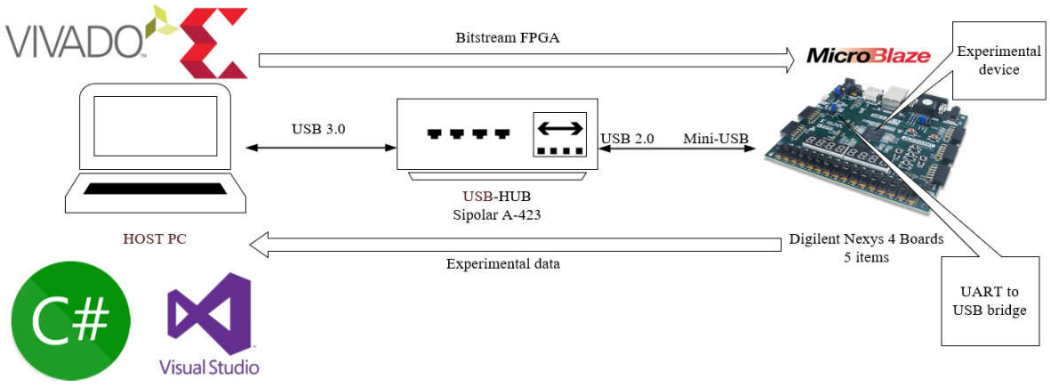

Рис. 5. Экспериментальная установка
Fig. 5. Experimental setup

Интерпретация данных эксперимента

Запись в файле данных эксперимента представляет собой значения двух счетчиков, которые соответствуют количеству зарегистрированных передних фронтов генерируемых импульсных последовательностей КО для каждого измерения. Опираясь на эти значения, а также на факт того, что КО генерирует сигнал в виде меандра, можно выразить величину задержки

$$D_i = \frac{D_s}{2N_i}, \quad (1)$$

где D_s – время работы КО;
N_i – значение счетчика для i-го измерения.

Согласно формуле (1) были рассчитаны значения задержек для каждого измерения. После этого для каждой конфигурации были вычислены характеристики математического ожидания, среднеквадратичного отклонения, относительной девиации и мод значений задержек двух КО, построенных на функционально симметричных путях FPGA. Полученные результаты представлены в табл. 1. Также для каждой конфигурации были найдены минимумы и максимумы задержек. Зависимость разницы значений минимума и максимума задержек для RO_1 и RO_2 Δ(Max, Min) от N представлена на рис. 6.

Таблица 1. Статистические характеристики задержек распространения через симметричные пути FPGA различной длины

Table 1. Statistical characteristics of propagation delays through symmetrical FPGA paths of various lengths

N	μ_1, нс	σ_1, нс	σ_1/μ_1, %	Mo_1, нс	μ_2, нс	σ_2, нс	σ_2/μ_2, %	Mo_2, нс
8	4,05	0,27	0,07	4,02	3,71	0,27	0,07	3,66
9	4,07	0,31	0,08	4	3,75	0,31	0,08	3,91
10	4,93	0,21	0,04	4,96	4,97	0,22	0,04	4,99
11	4,87	0,28	0,06	4,97	4,60	0,28	0,06	4,70
12	5,44	0,23	0,04	5,43	5,41	0,23	0,04	5,33
13	5,89	0,24	0,04	5,97	6,07	0,28	0,05	6,11
14	7,11	0,29	0,04	7,16	6,75	0,28	0,04	6,76
15	6,47	0,38	0,06	6,56	6,51	0,33	0,05	6,59
16	7,53	0,35	0,05	7,63	7,50	0,35	0,05	7,54
17	6,85	0,43	0,06	6,99	6,96	0,43	0,06	7,09
18	7,85	0,41	0,05	7,95	7,77	0,41	0,05	7,89
19	7,47	0,45	0,06	7,59	7,51	0,49	0,06	7,59
20	9,25	0,40	0,04	9,26	8,78	0,42	0,05	8,87
32	12,25	0,58	0,05	12,29	12,07	0,59	0,05	12,13
64	23,71	0,78	0,03	23,82	23,77	0,78	0,03	23,83
128	48,95	1,04	0,02	49,01	49,08	1,05	0,02	49,16

Согласно полученным результатам прослеживается увеличение окна значений задержек с увеличением N, что потенциально улучшает характеристики ФНФ.

Распределения временных задержек для всех исследуемых конфигураций были близки к нормальному. В качестве примера приводится график распределения временных задержек для конфигурации N = 128 (рис. 7).

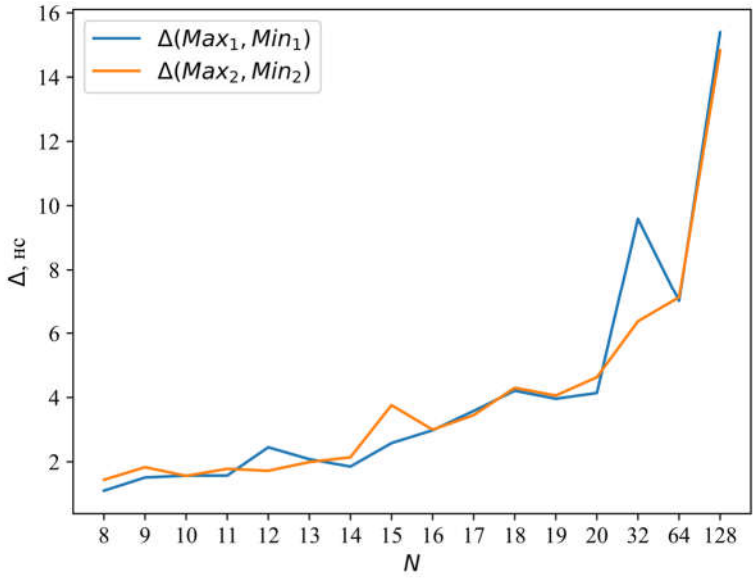

Рис. 6. Зависимость разниц максимального и минимального значения задержек от длины симметричных путей
Fig. 6. Dependence of the differences between the maximum and minimum values of delays on the length of symmetric paths

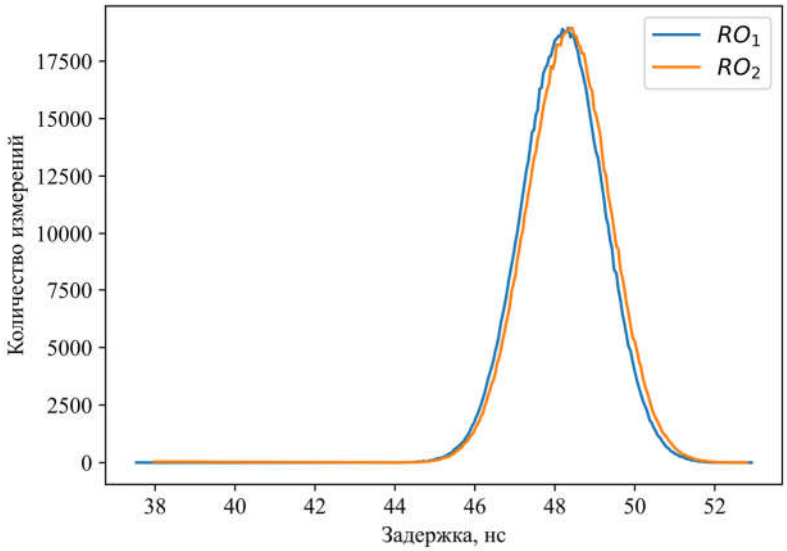

Рис. 7. Временное распределение задержек для конфигурации $N = 128$
Fig. 7. Time distribution of delays for configuration $N = 128$

Для оценки зависимости асимметричности распределения задержек от длины исследуемых путей был рассчитан коэффициент асимметрии Пирсона, график которого отображен на рис. 8.

График распределения задержек $N = 128$ демонстрирует практически идентичное распределение измерений для RO_1 и RO_2. Небольшой сдвиг графика RO_2 относительно RO_1 может быть обусловлен, например, большей задержкой петли обратной связи RO_2, т. к. эта часть RO является неизмененной при всех измерениях и вносит постоянную задержку. Для RO_1 и RO_2 величина этой задержки будет принципиально разной, но неизменной для всех измерений. Значения асимметрии распределений задержек имеют тенденцию снижения с увеличением значения N, что может свидетельствовать о потенциальном улучшении статистических характеристик ФНФ с ростом N.

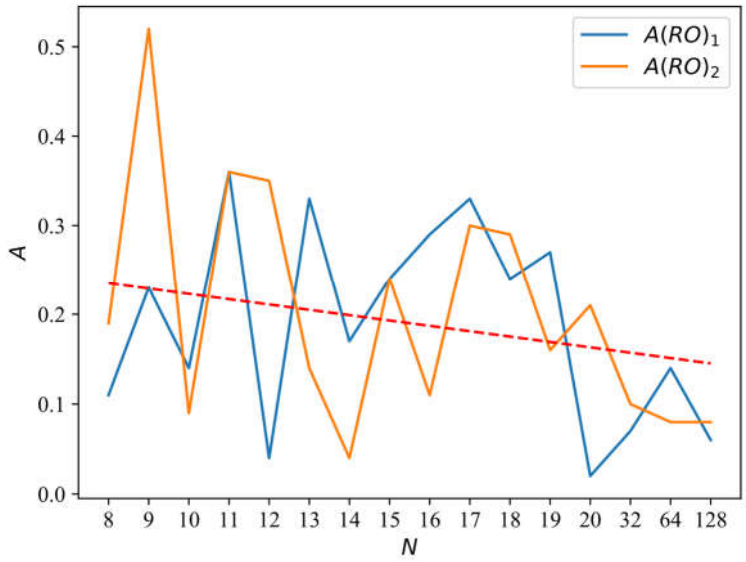

Рис. 8. Зависимость коэффициента асимметрии *A* распределения значений задержек от длины симметричных путей
Fig. 8. Dependence of the skewness coefficient (factor) *A* of the distribution of delay values on the length of symmetric path*s*

Затем были оценены взаимные значения двух счетчиков для конкретного измерения. Если значения оказывались равны, то измерения относилось к классу «*x*», если значение первого было меньше, чем значение второго счетчика, – к классу «1», и если наоборот – к классу «0». Поскольку измерения для конфигураций с длинами $N \in [8;20]$ проводились для всего множества запросов и эксперимент проводился на 5 устройствах и повторялся 10 раз, то сумма элементов всех классов измерения для каждой реализации должна быть равна $5*10*2^N$. В свою очередь для конфигураций с длинами $N \in \{32, 64, 128\}$ количество запросов было фиксированным и составляло $C = 10^6$. Полученные результаты отображены в виде гистограмм (рис. 9, 10).

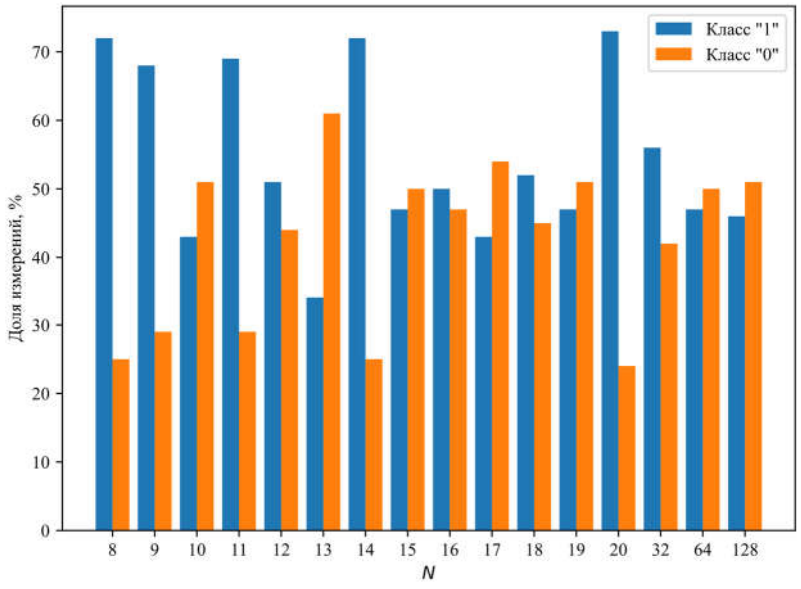

Рис. 9. Доля измерений классов «1» и «0»
Fig. 9. Percentage of measures of classes “1” and “0”

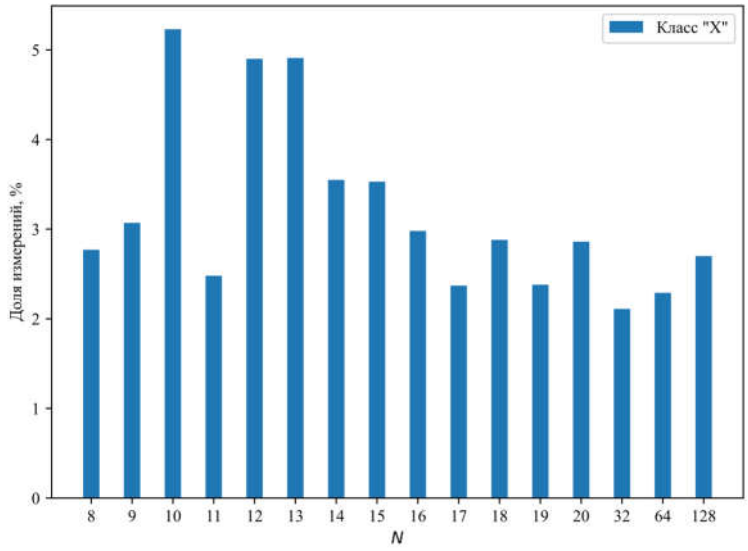

Рис. 10. Доля измерений класса «*x*»
Fig. 10. Percentage of measures of class "*x*"

Кроме этого, была рассчитана характеристика стабильности получаемых задержек, выраженная в доле стабильных измерений от общего количества. Под стабильным понимался такой запрос, при многократном повторении которого либо значения двух счетчиков постоянно совпадали, либо значение первого всегда было больше второго, либо наоборот (рис. 11).

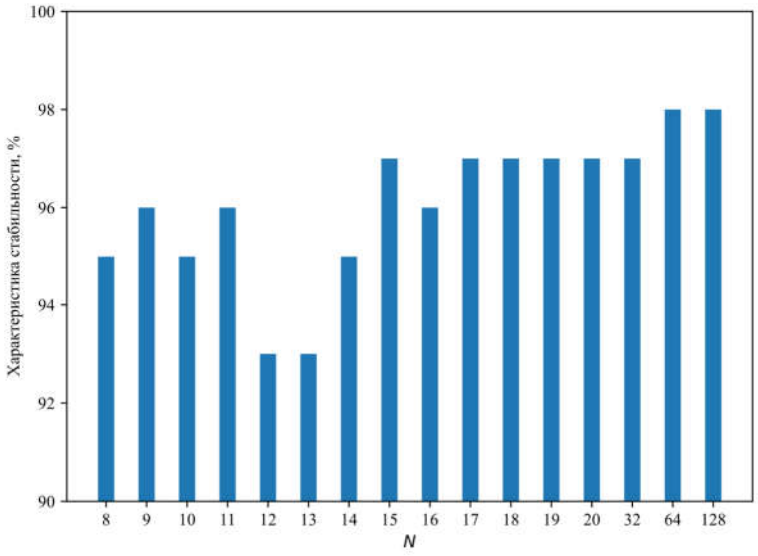

Рис. 11. Гистограмма характеристики стабильности
Fig. 11. Stability characteristic histogram

После сбора данных с нескольких плат, были рассчитаны значения характеристик уникальности. Причем уникальность оценивалась как отдельно для значений каждого счетчика (2), так и для разности их значений (4), а также уникальности результатов сравнения измерений для двух счетчиков и отнесения ответа к одному из трех классов при фиксированных запросах (5).

$$U = \frac{1}{C}\sum_{u=1}^{C} Uniq(R_{u0}, R_{u1}, ..., R_{um-1}), \quad (2)$$

где C – количество запросов; m – количество экземпляров; R_{um} – значение счетчика *Counter* при запросе с индексом u на экземпляре устройства с индексом m.

$$Uniq(\{Z\}) = \begin{cases} 1, \text{если все элементы множества } Z \text{ уникальны} \\ 0, \text{если имеется хотя бы два одинаковых элемента множества } Z \end{cases}. \quad (3)$$

$$U_{\Delta} = \frac{1}{C}\sum_{u=1}^{C} Uniq(\{\Delta(R_{1u0}, R_{2u0}),\ \Delta(R_{1u1},\ R_{2u1}),\ ...,\ \Delta(R_{1um-1}, R_{2um-1})\}), \quad (4)$$

где C – количество запросов; m – количество экземпляров; R_{1um} и R_{2um} – значения счетчиков $Counter_1$ и $Counter_2$ соответственно при запросе с индексом u на экземпляре устройства с индексом m.

$$U_{cmp} = \frac{1}{C}\sum_{i=1}^{C} \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} HD(CMP(R_{1iu}, R_{2u1}), CMP(R_{1iv}, R_{2iv})), \quad (5)$$

где C – количество запросов, m – количество экземпляров, R_{1im} и R_{2im} – значения счетчиков $Counter_1$ и $Counter_2$ соответственно при запросе с индексом i на экземпляре устройства с индексом m.

$$CMP(Value_0, Value_1) = \begin{cases} X, \text{если } Value_0 = Value_1 \\ 1, \text{если } Value_0 > Value_1 \\ 0, \text{если } Value_0 < Value_1 \end{cases}. \quad (6)$$

Расстояние Хэмминга HD для тернарных одноразрядных векторов определяется согласно табл. 2.

Таблица 2. Расстояние Хэмминга для тернарных одноразрядных векторов
Table 2. Hamming distance for ternary one-bit vectors

Значение	0	1	X
0	0	1	0,5
1	1	0	0,5
X	0,5	0,5	0

Полученные метрики уникальности абсолютных значений измерений для всех исследуемых конфигураций симметричных путей АФНФ $U(RO_1)$ и $U(RO_2)$ составили 0,99. Характеристика уникальности значений разниц измерений для двух счетчиков при фиксированных запросах U_{Δ} оказалась равна 0,78. Метрика уникальности отнесения взаимных значений счетчиков к классам «1», «0» либо «x» U_{cmp} имела значение 0,01.

Заключение

Полученные результаты подтверждают зависимость характеристик задержек распространения сигналов по симметричным путям на ИС от количества составных элементов. Абсолютные значения математического ожидания, статистических мод, максимума и минимума измеренных задержек линейно возрастают с увеличением количества звеньев N. Также при увеличении N повышаются значения СКО и увеличивается стабильность измерений. Асимметрия значений статистических характеристик для двух независимых КО одной конфигурации подтверждает тезис о невозможности построения идеально симметричных путей на FPGA [11]. Кроме этого, уменьшается разность между количеством измерений, отнесенных к классам «больше» и «меньше», что потенциально повышает случайность ФНФ, а также снижается доля измерений класса «равны». Рассчитанные характеристики межкристальной уникальности свидетельствуют о высокой уникальности абсолютных значений задержек при фиксированных запросах от устройства к устройству, а также уникальности значений их разностей. Однако при использовании схемы выработки ответа, аналогичной классической АФНФ, основанной на фиксации разниц прохождения фронтов тестовых сигналов через симметричные пути с использованием в качестве арбитра D-триггера, и последующего расчета метрики уникальности значения оказались крайне низкими (около 1 %). Это говорит о потенциально низкой межкристальной уникальности классической АФНФ, построенной

с соответствующей длиной путей для данной технологии. Потенциально ФНФ, построенные на основе симметричных путей с большим количеством элементов, будут обладать лучшими свойствами по сравнению с аналогичными ФНФ с меньшим количеством элементов.

В дальнейшем планируется продолжить исследования временных параметров симметричных путей АФНФ. В частности, провести аналогичные эксперименты на других платах с другими кристаллами FGPA, изучить влияние размера окна измерений на получаемые значения. Также для анализа задержек распространения сигналов по пути цифрового перспективным представляется применение подходов, используемых при построении времяизмерительных систем TDC (time to digital converter).

Список литературы

1. Agarwal A., Blaauw D., Zolotov V. Statistical Timing Analysis for Intra-Die Process Variations with Spatial Correlations. ICCAD-2003. International Conference on Computer Aided Design. 2003:900-907. DOI: 10.1109/ICCAD.2003.159781.
2. Böhm C., Hofer M. Physical Unclonable Functions in Theory and Practice. New York: Springer Science+Business Media; 2013.
3. Wang Y., Wang C., Gu C. Theoretical Analysis of Delay-based PUFs and Design Strategies for Improvement. 2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019:1-5. DOI: 10.1109/ISCAS.2019.8702722.
4. Rührmair U., Schröder H., Katzenbeisser S. Strong PUFs: Models, Constructions, and Security Proofs. Towards Hardware-Intrinsic Security. 2010:79-96. DOI: 10.1007/978-3-642-14452-3_4.
5. Lee J.W., Lim D., Gassend B. A technique to build a secret key in integrated circuits for identification and authentication applications. Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525). 2004:176-179. DOI: 10.1109/VLSIC.2004.1346548.
6. Ozturk E., Hammouri G., Sunar B. Physical unclonable function with tristate buffers. 2008 IEEE International Symposium on Circuits and Systems. 2008:3194-3197. DOI: 10.1109/ISCAS.2008.4542137.
7. Chen Q., Csaba G., Lugli P. The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions. 2011 IEEE International Symposium on Hardware-Oriented Security and Trust. 2011:134-141. DOI: 10.1109/HST.2011.5955011.
8. Suh G.E., Devadas S. Physical unclonable functions for device authentication and secret key generation. Proceedings of the 44th annual Design Automation Conference. 2007:9-14. DOI: 10.1145/1278480.1278484.
9. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонируемые функции. Информатика. 2011;2(30):92-103.
10. Иванюк А.А., Заливако С.С. Физическая криптография и защита цифровых устройств. Доклады БГУИР. 2019;2(120):50-58.
11. Yu H., Xu Q., Leong P.H.W. Fine-grained characterization of process variation in FPGAs. 2010 International Conference on Field-Programmable Technology. 2010:138-145. DOI: 10.1109/FPT.2010.5681770.

References

1. Agarwal A., Blaauw D., Zolotov V. Statistical Timing Analysis for Intra-Die Process Variations with Spatial Correlations. ICCAD-2003. International Conference on Computer Aided Design. 2003:900-907. DOI: 10.1109/ICCAD.2003.159781.
2. Böhm C., Hofer M. Physical Unclonable Functions in Theory and Practice. New York: Springer Science+Business Media; 2013.
3. Wang Y., Wang C., Gu C. Theoretical Analysis of Delay-based PUFs and Design Strategies for Improvement. 2019 IEEE International Symposium on Circuits and Systems (ISCAS). 2019:1-5. DOI: 10.1109/ISCAS.2019.8702722.
4. Rührmair U., Schröder H., Katzenbeisser S. Strong PUFs: Models, Constructions, and Security Proofs. Towards Hardware-Intrinsic Security. 2010:79-96. DOI: 10.1007/978-3-642-14452-3_4.
5. Lee J.W., Lim D., Gassend B. A technique to build a secret key in integrated circuits for identification and authentication applications. Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat No.04CH37525). 2004:176-179. DOI: 10.1109/VLSIC.2004.1346548.
6. Ozturk E., Hammouri G., Sunar B. Physical unclonable function with tristate buffers. 2008 IEEE International Symposium on Circuits and Systems. 2008:3194-3197. DOI: 10.1109/ISCAS.2008.4542137.
7. Chen Q., Csaba G., Lugli P. The Bistable Ring PUF: A new architecture for strong Physical Unclonable

Functions. 2011; IEEE International Symposium on Hardware-Oriented Security and Trust. 2011:134-141. DOI: 10.1109/HST.2011.5955011.
8. Suh G.E., Devadas S. Physical unclonable functions for device authentication and secret key generation. Proceedings of the 44th annual Design Automation Conference. 2007:9-14. DOI: 10.1145/1278480.1278484.
9. Yarmolik V.N., Vashinko Y.G. [Physical unclonable functions]. Informatika = Informatics. 2011;2(30):92-103. (In Russ.)
10. Ivaniuk A.A., Zalivaka S.S. [Physical cryptography and security of digital devices]. Doklady BGUIR=Doklady BGUIR. 2019;2(120):50-58. (In Russ.)
11. Yu H., Xu Q., Leong P.H.W. Fine-grained characterization of process variation in FPGAs. 2010 International Conference on Field-Programmable Technology. 2010:138-145. DOI: 10.1109/FPT.2010.5681770.

Вклад авторов

Шамына А.Ю. провел экспериментальные исследования, проанализировал и обобщил полученные результаты.

Иванюк А.А. осуществил постановку задачи для проведения исследования.

Authors contribution

Shamyna A.Yu. conducted experimental studies, analyzed, and summarized the results.

Ivaniuk A.A. carried out the formulation of the problem for the study.

Сведения об авторах

Шамына А.Ю., м.т.н., старший преподаватель Белорусского государственного университета информатики и радиоэлектроники.

Иванюк А.А., доктор технических наук, доцент, профессор кафедры информатики, заведующий совместной учебной лабораторией «СК хайникс мемори солюшнс Восточная Европа» Белорусского государственного университета информатики и радиоэлектроники.

Information about the authors

Shamyna A.Yu., M.Sci., (Engineering), Senior Lecturer at the Belarusian State University of Informatics and Radioelectronics.

Ivaniuk A.A., Dr. of Sci. (Engineering), Associate Professor, Professor at the Comp. Sci. Department, Head of the Joint Educational Laboratory “SK hynix memory solutions Eastern Europe” of the Belarusian State University of Informatics and Radioelectronics.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6,
Белорусский государственный университет информатики и радиоэлектроники;
тел + 375-17-293-84-63;
e-mail: shamyna@bsuir.by, ivaniuk@bsuir.by
Шамына Артем Юрьевич

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki, 6,
Belarusian State University
of Informatics and Radioelectronics;
tel. +375-17-293-84-63;
e-mail: shamyna@bsuir.by, ivaniuk@bsuir.by
Shamyna Artsiom Yurievich