http://dx.doi.org/10.35596/1729-7648-2022-20-4-71-79

Оригинальная статья
Original paper

УДК 681.324

ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ ТИПА АРБИТР С ЗАВЕДОМО АСИММЕТРИЧНЫМИ ПАРАМИ ПУТЕЙ

В.Н. ЯРМОЛИК, А.А. ИВАНЮК

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

Поступила в редакцию 23 декабря 2021

Аннотация. Анализируются методы построения физически неклонируемых функций (ФНФ), являющихся основной физической криптографии. Отмечается широкая применимость ФНФ типа арбитр, основанных на анализе задержек сигнала, передаваемого по двум путям. Показывается, что случайность величин задержек объясняется технологическими вариациями при изготовлении ФНФ, а их зависимость – применением однородных повторяющихся элементов, обеспечивающих симметрию путей. Как альтернатива существующим решениям в статье предлагается новый подход для построения ФНФ типа арбитр на базе заведомо асимметричных путей. В качестве источников случайности рассматриваются задержки логических элементов, показывается их многообразие и отличительные характеристики в зависимости от количества входов, на которые подается активный сигнал, и от значений на остальных входах. Предлагается методика балансировки множества пар путей ФНФ типа арбитр, заключающаяся в регулировании длительности импульсного тестового сигнала в зависимости от четырех видов асимметрии путей. Предлагаются новые структуры ФНФ типа арбитр с асимметричными парами путей. Экспериментальные исследования подтверждают возможность использования различных источников случайности в виде задержек сигнала логическими элементами.

Ключевые слова: физическая криптография, физически неклонируемые функции типа арбитр, логический элемент, временная задержка логического сигнала.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Ярмолик В.Н., Иванюк А.А. Физически неклонируемые функции типа арбитр с заведомо асимметричными парами путей. Доклады БГУИР. 2022; 20(4): 71-79.

ARBITER PHYSICAL UNCLONABLE FUNCTIONS WITH ASYMMETRIC PAIRS OF PATHS

VYACHESLAV N. YARMOLIK, ALEXANDER A. IVANIUK

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

Submitted 23 December 2021

Abstract. The methods of constructing physical unclonable functions (PUF), which are the basis of physical cryptography, are analyzed. The broad applicability of the Arbiter PUF, based on the analysis of the delays of the signal transmitted along two paths, is noted. It is shown that the randomness of the delays is explained by technological variations in the manufacturing process of PUF and their dependence on the use of homogeneous repeating elements that ensure the symmetry of the paths. As an alternative to the existing solutions, the article proposes a new approach for constructing an Arbiter PUF based on asymmetric paths. The sources of randomness as logical element delays are investigated. Their diversity and distinctive characteristics are shown depending on the number of inputs to which an active signal is supplied and the values at other inputs. A technique for balancing a set of pairs of paths of Arbiter PUF is proposed, which lays in regulating the duration of the impulse test signal depending on four types of path asymmetry. New structures of Arbiter PUF with asymmetric pairs of paths are proposed. Experimental studies confirm the possibility of using various sources of randomness in the form of signal delays.

Keywords: physical cryptography, arbiter physical unclonable functions, logic element, time delay of a logic signal.

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

For citation. Yarmolik V.N., Ivaniuk A.A. Arbiter Physical Unclonable Functions with Asymmetric Pairs of Paths. Doklady BGUIR. 2022; 20(4): 71-79.

Введение

Первое упоминание о физически неклонируемых функциях было сформулировано R. Pappu в 2001 году в работе [1] при определении физически однонаправленных функций (Physical One-Way Functions). Близкие решения, практически в то же время, предложил B. Gassend и др. при реализации кремниевых физически случайных функций (Physical Random Functions) [2]. Указанные результаты были получены исторически первыми, однако в настоящее время в основном употребляется понятие физически неклонируемых функций (ФНФ), происходящее от англоязычного словосочетания Physical Unclonable Functions (PUF).

Основным свойством ФНФ является их неклонируемость, которая достигается тем, что в процессе изготовления ФНФ невозможно создать два идентичных цифровых устройства, обладающих одинаковыми характеристиками. Вариации значений характеристик цифровых устройств обусловлены случайными колебаниями различного рода примесей в используемых материалах, геометрией и размерами линий соединений и компонент (транзисторов, сопротивлений) элементов и другими факторами, влияние на которые со стороны изготовителя затруднено либо вообще невозможно. Эти фундаментальные источники вариаций вызывают изменения в значениях характеристик элементов цифровых устройств, и в особенности их временных задержек [3, 4].

В общем случае ФНФ описываются значениями входных и соответствующих им выходных параметров (сигналов). Подобная пара, состоящая из входного физического параметра запроса (Challenge (C)) и выходного параметра ответа (Response (R)), называется парой запрос-ответ (Challenge-Response Pair (CRP)), рассматриваемой как функция R = F(C) [3, 4]. Исторически первыми ФНФ являются физически неклонируемые функции типа арбитр АФНФ (Arbiter PUF), предложенные в 2002 году [5]. АФНФ оказались весьма удачным решением, основанным на различии задержек прохождения сигнала через симметричные пути цифровых устройств. На сегодняшний день существует большое множество схем АФНФ, которые отличаются как своей структурой [3−5] и областью применения [4−7], так и практической реализацией [3, 7]. При этом различие задержек сигналов является основным фактором, влияющим на свойства АФНФ. Классическая методология построения АФНФ основана на использовании пар симметричных путей. Причем симметрия пар путей во многих разновидностях ФНФ подобного вида является обязательным условием.

Основным недостатком симметрии при создании пар путей является формирование по двум путям случайных времен задержки, которые формируются при максимально идентичных условиях, чем и предопределяется их взаимная зависимость. Одинаковые условия и ограничения при получении двух случайных величин задержек негативно сказываются на свойствах АФНФ. В данной статье предлагается новый подход к построению АФНФ, который, по сравнению с известными решениями, основан на использовании заведомо несимметричных пар путей, что позволяет улучшить свойства АФНФ и их стабильность.

Анализ задержек логических элементов

При разработке различных схемотехнических решений по созданию ФНФ ключевым фактором является задержка прохождения сигнала через логический элемент. Считается, что задержка сигнала, как правило, импульсного, принимает случайное, непредсказуемое значение в рамках определенного временного интервала. Данный интервал, либо среднее значение задержки, для каждого логического элемента зависит от типа использованных в нем электронных компонент (ТТЛ, КМОП, ЭСЛ и др.), принципиальной схемы элемента, и особенностей технологического процесса его изготовления.

Главная парадигма большинства работ по ФНФ состоит в том, что изначально принимается гипотеза о фиксированном значении задержки через элемент без учета многих факторов. Эта задержка в процессе изготовления принимает случайное значение, которое остается неизменным в процессе использования ФНФ. Единственными факторами, влияющими на задержку сигнала и обсуждаемыми авторами работ по ФНФ, являются внешние факторы, такие как температура, давление, электромагнитные излучения и др., а также временной фактор, влияющий на деградацию физических и химических свойств материалов, используемых для изготовления элемента.

Придерживаясь данной парадигмы, следует отметить, что результатом изготовления даже простейшего логического элемента, такого как повторитель или инвертор, будет являться как минимум два значения задержек, принимающих произвольные значения из диапазона возможных их величин. Значения задержек фронтов (переходов) логического сигнала из 0 в 1 (Low to High (LH)) – передний фронт, либо из 1 в 0 (High to Low (HL)) – задний фронт, как правило, отличаются и в сильной степени зависят от типа электронных элементов, используемых для их изготовления. Величины этих задержек определяются на уровне 50 % размаха входного и выходного сигналов и обозначаются как Δ(LH) и Δ(HL) [8]. Обобщая значения двух задержек Δ(LH) и Δ(HL), для произвольного логического элемента определяется средняя их величина $\Delta_G = (\Delta(\text{LH}) + \Delta(\text{HL}))/2$, которая и используется при анализе и синтезе ФНФ. Большинство рассуждений авторов о случайности величины задержки через элемент либо путь оперирует задержкой Δ_G.

Исследования задержек на логических элементах чаще всего рассматриваются в режиме переключения сигнала по одному входу элемента (Single Input Switching (SIS)), изменения которого приводят к изменению выходного значения [2, 3]. Результаты исследований, приведенные в работе [8], показывают однозначную зависимость задержки прохождения сигнала через логические элементы в зависимости от активного входа, т. е. входа, на который подается активный сигнал, приводящий к изменению значения сигнала на выходе элемента. Более сложные процессы и, соответственно, зависимости задержек через логический элемент возникают в случае переключения сигналов одновременно по нескольким входам (Multi Input Switching (MIS)) [8]. Например, при одновременном переключении сигналов из 1 в 0 и, наоборот, из 0 в 1 по обоим входам двухвходового логического элемента. В общем случае показано, что, если выход m-входового КМОП логического элемента И-НЕ работает на нагрузочную емкость C_{Load}, задержка Δ(LH) распространения сигнала зависит от количества активных входов [8]. При переключении логического значения только по одному входу величина задержки Δ(LH) в m раз больше по сравнению со случаем переключения по всем m его входам. Таким образом, задержка сигнала через логический элемент зависит от пути прохождения сигнала, который определяется активным входом/входами и логическими значениями на неактивных входах/входе, а также самим входным сигналом.

На примере простейших двухвходовых элементов 2И и 2XOR с входами In1, In2 и выходом Out, рассмотрим многообразие задержек сигнала, которые в процессе изготовления принимают случайные значения и могут быть использованы при построении АФНФ.

Табл. 1 содержит описания задержек сигнала на элементах 2И и 2XOR в режиме SIS. Например, Δ_1(LH) для элемента 2XOR представляет собой задержку изменения сигнала из 0 в 1 (LH) на выходе Out при изменении входного In1 сигнала из 0 в 1 (LH) и удержании на втором входе In2 логической 1. Как видно из приведенной табл. 1, элемент 2И генерирует четыре задержки, а 2XOR восемь различных задержек, принимающих случайные значения. Элемент 2И является источником еще двух задержек, которые формируются в режиме MIS. При одновременном изменении LH или HL по входам In1 и In2 элемента 2И на его выходе Out будет происходить аналогичное изменение сигнала LH или HL.

Таблица 1. Задержки сигнала на элементах 2И и 2XOR
Table 1. Signal delays on the 2AND and 2XOR elements

2И (2AND)				2XOR							
Задержка Delay	In1	In2	Out	Задержка Delay	In1	In2	Out	Задержка Delay	In1	In2	Out
Δ_1(LH)	LH	1	LH	Δ_1(LH)	LH	0	LH	Δ_5(HL)	HL	0	HL
Δ_2(HL)	HL	1	HL	Δ_2(HL)	LH	1	HL	Δ_6(LH)	HL	1	LH
Δ_3(LH)	1	LH	LH	Δ_3(LH)	0	LH	LH	Δ_7(HL)	0	HL	HL
Δ_4(HL)	1	HL	HL	Δ_4(HL)	1	LH	HL	Δ_8(LH)	1	HL	LH

Использование случайного значения задержки сигнала при проектировании пути АФНФ, без учета его специфики и особенностей, может приводить к наличию закономерностей и, соответственно, ухудшению вероятностных свойств АФНФ. С другой стороны, учет и использование детерминированных зависимостей задержек сигнала через элемент может существенно увеличить разброс этих задержек и, соответственно, увеличить стабильность функционирования АФНФ. Теория и практика по созданию ФНФ, в том числе и АФНФ, состоит в одновременном обеспечении приемлемого уровня вероятностных свойств при одновременном сохранении достаточной стабильности функционирования [3−7].

Построение ФНФ типа арбитр

В общем случае при реализации АФНФ изготавливаются два функционально и топологически идентичных электрических пути, представляющих собой последовательно подключенные элементы и их межсоединения. Очевидно, что оба пути будут иметь близкие значения величин задержек распространения по ним сигналов, однако они будут принципиально разными в силу технологических вариаций в процессе производства. Процедура измерения задержек заключается в одновременной подаче на входы обоих путей сигнала и определении, на выходе которого из них сигнал появится быстрее. Классической схемой ФНФ типа арбитр является схема, состоящая из n последовательно подключенных пар двухвходовых мультиплексоров (MUX) [3, 4, 7]. Адресные входы обоих мультиплексоров MUX_1 и MUX_2 каждой пары объединяются и используются в качестве одного из входов для задания значения бита $c_j \in \{0, 1\}$, $j \in \{0, 1, 2, \ldots, n-1\}$, запроса C, принимающего одно из 2^n возможных значений. Запрос C в схеме АФНФ формирует два пути таким образом, что если $c_j = 0$ для j-й ступени АФНФ, то для построения первого пути используется мультиплексор MUX_1, а для второго – MUX_2, а при $c_j = 1$ – наоборот. Каждая пара путей имеет общий вход, а выходы первого и второго пути подключены соответственно к D входу D-триггера и к его синхронизирующему входу Clk. В случае АФНФ D-триггер является арбитром и перед проведением эксперимента устанавливается в исходное состояние, например, нулевое. Для конкретного запроса C генерируется ответ $R \in \{0, 1\}$ как результат эксперимента по определению, по какому из путей выбранной запросом C пары путей (первому или второму) задержка входного сигнала меньше [3, 4, 7].

При формировании пары путей с различными значениями задержек все из n пар мультиплексоров MUX_1 и MUX_2 вносят свои задержки в каждый из путей. Двухвходовой мультиплексор MUX_1, также как и MUX_2, является источником двух случайных величин задержки сигнала в зависимости от используемого его информационного входа, определяемого битом запроса c_j. В силу топологических и физических особенностей изготовления цифровых устройств можно считать, что значения двух случайных задержек, полученных на одном мультиплексоре, имеют существенно большую взаимную зависимость, чем две случайные величины, полученные из различных физических источников (MUX_1 и MUX_2). Важно отметить, что если MUX_1 используется для построения первого пути, то MUX_2 – для второго, и наоборот, в зависимости от значения бита запроса, что и является методологической основой выравнивания задержек сигнала по двум путям [3−7].

Как альтернатива известным решениям при создании АФНФ, предлагается подход для построения АФНФ с изменяемыми задержками без переключения путей. В отличие от классических схем АФНФ, бит запроса определяет (выбирает) только значение задержки

по каждому пути, через базовый элемент пути. Два пути заранее определены последовательным подключением базовых элементов, примеры которых приведены на рис. 1. В данном случае выбирается не пара путей, как это реализуется в классических АФНФ, а величины задержек по двум независимым путям. Например, для двухвходовых мультиплексоров (рис. 1, *a*) значение бита запроса определяет вход мультиплексора, по которому тестовый сигнал передается на его выход, выбирая таким образом одно из возможных значений задержек сигнала. Применение элементов 2XOR также позволяет выбирать одно из двух значений задержки по заранее построенным двум путям, но уже по другому принципу (рис. 1, *b*). Формирование 0 или 1 по второму входу XOR в виде запроса c_j управляет (выбирает одно из двух значений) задержкой по первому входу.

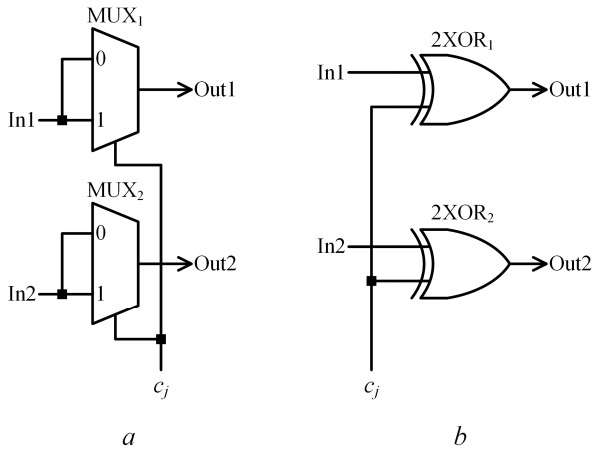

Рис. 1. Базовые элементы для построения АФНФ
Fig. 1. Basic elements for building an APUF

И в первом (рис. 1, *a*), и во втором случаях (рис. 1, *b*) значение запроса $C = c_0, c_1, c_2 \ldots, c_{n-1}$ определяет временную задержку прохождения сигнала по каждому из двух путей АФНФ, построенной из n последовательно соединенных базовых элементов. В качестве базовых элементов для построения АФНФ могут использоваться и другие элементы с разным количеством входов, например, мультиплексоры или элементы XOR, но с большим количеством входов.

Построение АФНФ с двумя физически независимыми путями и управляемыми задержками прохождения сигнала по ним улучшает их вероятностные свойства за счет уменьшения зависимости величин задержек по двум путям. Однако физическая независимость двух путей как источника двух случайных величин может приводить к их асимметрии, когда один из путей может оказаться быстрее второго для большинства значений запроса C, следовательно, одно из значений ответов R будет преобладать над другим. Асимметрия путей требует их балансировки, заключающейся в выравнивании задержек по обоим путям.

Балансировка путей АФНФ

С учетом девиации задержки для конкретного пути, в зависимости от запроса C, можно определить диапазон Δ ее изменения как разницу между максимальной и минимальной величинами задержки. Идеальным является случай, когда среднее значение задержки по первому пути равняется такому же значению по второму пути, диапазон Δ разброса значений задержек по обоим путям велик, а сами задержки представляют собой случайные независимые значения. Упрощенно это показано на рис. 2, *a* в виде девиации фронтов тестового импульса, одновременно поданного на входы обоих путей и прошедшего эти пути с конкретными задержками. Условно первый путь обозначается символом *D*, а второй – обозначается как *Clk*, что соответствует обозначениям входов *D*-триггера, выступающего в роли арбитра. Выход Out1 (см. рис. 1) первого пути подключается к *D* входу арбитра, а Out2 второго – ко входу *Clk*. Процедура арбитража выполняется во временном интервале, определяемом диапазоном Δ, в котором соотношение передних фронтов тестового импульса и определяет

значение ответа *R*. В идеальном случае переходы из нуля в единицу на выходах путей должны происходить в одном и том же временном диапазоне (см. рис. 2, *a*).

Приведенное требование является идеализированным и на практике, как правило, недостижимо. Чаще встречаются ситуации, когда диапазоны фронтов, в рассмотренном случае передних фронтов импульса, по обоим путям для всех значений запросов не пересекаются либо лишь частично пересекаются. Это означает, что ответ *R* на любой запрос всегда будет один и тот же, либо какой-то из них, 0 или 1, будет заметно преобладать. На рис. 2 приведены четыре вида асимметрии. Для 1, 2 и 4 видов асимметрии, представленных соответственно на рис. 2, *b*, *c* и *e*, ответ *R* для любого запроса *C* всегда принимает значение 0. При наличии асимметрии третьего типа, показанной на рис. 2, *d*, ответ равняется 1.

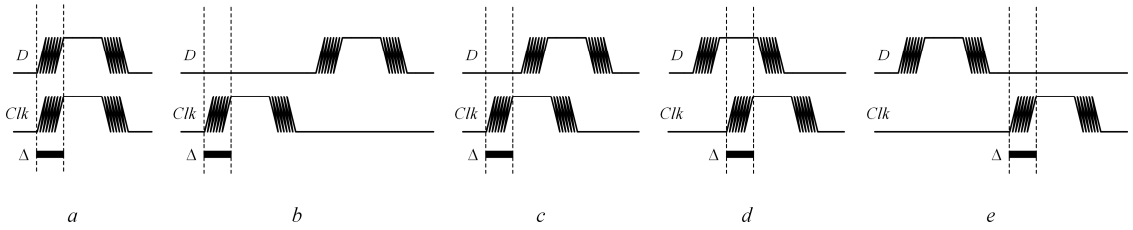

Рис. 2. Девиация задержек по двум путям: *a* – симметричный случай; *b*, *c*, *d*, *e* – случаи асимметрии
Fig. 2. Delay deviation along two paths: *a* – symmetric case; *b*, *c*, *d*, *e* – cases of asymmetry

Примеры асимметрии путей ФНФ типа арбитр показывают необходимость выравнивания задержек по множеству пар путей (балансировки путей), генерируемых запросами *C*, которое выполняется настройкой параметров тестовых сигналов. В качестве основных инструментов для балансировки необходим генератор перехода сигнала из нуля в единицу (LH) и генератор импульсных тестовых сигналов с изменяемой длительностью импульса. Кроме того, в качестве арбитра применяется *D*-триггер с управляемым входом синхронизации, который выполняет запись информации по положительному фронту (LH) в одном режиме, а по отрицательному (HL) – во втором. Не нарушая симметрии путей, по обоим входам классического *D*-триггера, используемого в качестве арбитра, подключаются элементы 2XOR. Элемент 2XOR по *D* входу триггера выполняет функцию повторителя, а по *Clk* входу – повторителя для обеспечения синхронизации в режиме LH и инвертора в режиме HL.

Сама процедура балансировки будет состоять из двух этапов. Первый этап заключается в определении типа асимметрии пар путей, а второй – непосредственно в балансировке задержек путей. Тип асимметрии первоначально определяется по результатам генерирования тестового сигнала, формирующего переход LH для различных запросов. В случае наличия одного из четырех типов асимметрии для всех запросов будет сформирован повторяющийся ответ 0 или 1. Нулевое значение ответа свидетельствует о том, что путь, подключенный к входу *Clk* арбитра, имеет меньшую задержку из двух путей, определенных запросом. Для импульсного тестового сигнала рассматриваются два режима: один – для записи ответа по переднему фронту импульса (LH), а второй – по заднему (HL). Результаты, полученные при подаче тестовых сигналов для определения типа асимметрии пар путей, формируемых запросами, приведены в табл. 2.

Таблица 2. Результаты тестирования пар путей при определении типа их асимметрии
Table 2. Results of path pairs testing when determining the type of their asymmetry

Тестовый сигнал Test signal		Тип асимметрии / Asymmetry type			
		1	2	3	4
Переход LH		0	0	1	1
Импульс	LH	0	0	1	0
	HL	0	1	0	0

Как видно из приведенной таблицы, все четыре типа асимметрии различимы и однозначно идентифицируются по результату процедуры определения типа асимметрии. Процедура балансировки путей заключается в изменении длительности (увеличении или уменьшении) тестового импульса. Это необходимо для совмещения временных интервалов изменения сигналов на обоих входах *D*-триггера. По сути, достигается такая же ситуация,

как и для идеального случая, проиллюстрированного на рис. 2, *a*, когда переключения на *D* входе триггера и его управляющем входе *Clk* происходят в одном временном диапазоне.

Устранение асимметрии достигается путем совмещения различных фронтов одного и того же импульса, проходящего по двум путям. Например, для асимметрии второго типа с уменьшением длительности импульса временной интервал LH по первому пути (*D*) совмещается с временным интервалом HL по второму пути (*Clk*), как это показано на рис. 3, *a*.

Второй пример на этом же рисунке иллюстрирует балансировку путей для четвертого типа асимметрии путем увеличения длительности тестового импульса. В этом случае совмещается временной диапазон изменения HL сигнала по первому пути с временным интервалом изменений LH по второму пути.

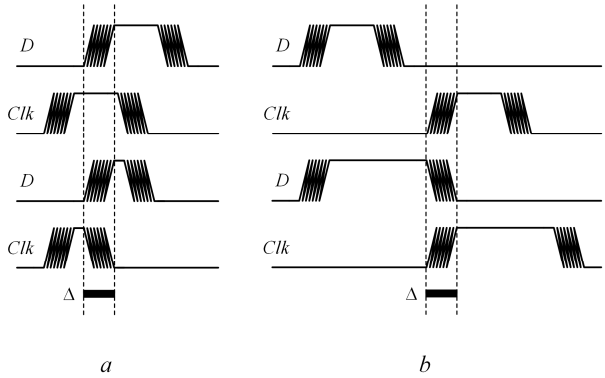

Рис. 3. Балансировка путей: *a* – для второго типа асимметрии; *b* – для четвертого типа асимметрии
Fig. 3. Balancing paths: *a* – for the second type of asymmetry; *b* – for the fourth type of asymmetry

Экспериментальная часть

Для подтверждения гипотезы, выдвинутой авторами, о различных задержках на элементах в режиме SIS была спроектирована схема, состоящая из 8 последовательно подключенных элементов 2XOR, охваченных обратной связью, что представляет собой кольцевой осциллятор [3, 4]. Кроме того, в цепи обратной связи был реализован дополнительный элемент 2И, обеспечивающий «старт/стопный» режим генератора. Для обеспечения генерирования импульсов на свободные входы элементов 2XOR необходимо подать запрос *C* с нечетным числом единиц. При этом период генерируемой импульсной последовательности будет зависеть от конкретного значения запроса. Для оценки численных значений периодов была спроектирована аппаратно-программная система на основе платы быстрого прототипирования Digilent Zybo Z7 с программируемой логической интегральной схемой (ПЛИС) Xilinx Zynq XC7Z010-1CLG400C.

В ходе первого эксперимента были оценены значения периодов $P(C_i)$ генерируемых сигналов при всех запросах C_i, удовлетворяющих условию $w(C_i) = 2k - 1, \forall\ k = 1, \ldots, n/2$, где w – вес Хемминга вектора запроса C_i. Анализ полученных данных свидетельствует о различии всех полученных значений $P(C_i)$, что подтверждает значимость и неравенство задержек Δ(LH) и Δ(HL) для элементов 2XOR.

В ходе второго эксперимента была подтверждена гипотеза об асимметрии двух путей для ФНФ типа арбитр и необходимости балансировки подобных путей. Для этого на одном кристалле ПЛИС были размещены два идентичных генератора из первого эксперимента с общим управлением и общей входной шиной запросов *C*. Как и в предыдущем эксперименте, были оценены зависимости значений периодов $P1(C_i)$ и $P2(C_i)$ сигналов, вырабатываемых двумя генераторами, от подаваемых на их входы значений запросов C_i. На рис. 4 приведены значения периодов $P1(C_i)$ и $P2(C_i)$ и значения их математических ожиданий μ1 и μ2 для всех *C*.

Если предположить, что первый генератор представляет собой путь АФНФ, который подключен к *D* входу арбитра, а второй – к *Clk* входу, то это будет соответствовать асимметрии третьего типа (см. рис. 3). При этом ширина диапазона изменения периода $P1(C_i)$ составляет 0,133 нс, а периода $P2(C_i)$ – 0,115 нс, и эти диапазоны не пересекаются.

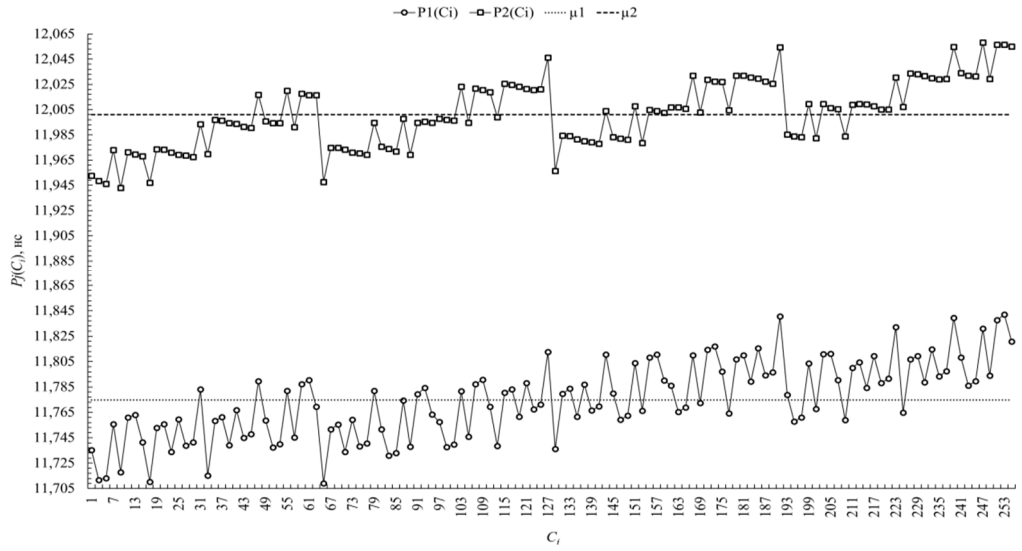

Рис. 4. Графики зависимостей $P1(C_i)$ и $P2(C_i)$
Fig. 4. $P1(C_i)$ and $P2(C_i)$ dependency plots

Отклонения от значений μ1 и μ2 и определяют значения суммарных задержек на всех структурных элементах генераторов в зависимости от значения запроса. Вычтем из полученных данных $P1(C_i)$ и $P2(C_i)$ для двух генераторов значения μ1 и μ2 соответственно и оценим разницу полученных величин, которая будет характеризовать различия уникальных элементов 2XOR двух путей. По сути, описанная математическая операция соответствует предложенному подходу к балансировке ассиметричных путей. Введем значение разницы задержек сигналов для двух путей: $Delta(P1,P2) = (P1(C_i)-\mu1)-(P2(C_i)-\mu2)$. Тогда все значения $Delta(P1,P2)$ можно разделить на три подмножества: практически одинаковые значения $-0{,}000834765 \le Delta(P1,P2) \le 0{,}00058$ нс; устойчиво положительные значения $Delta(P1,P2) \ge 0{,}0013$ нс; устойчиво отрицательные значения $Delta(P1,P2) \le -0{,}0021$ нс.

Таким образом, результат сравнения двух путей можно представить в виде трех символов (ответов в контексте классических ФНФ типа арбитр): ‘X’ – метастабильное значение, означающее максимально близкие значения $P1(C_i)$ и $P2(C_i)$; ‘1’ – стабильное единичное значение, которое интерпретируется как различимая разница между двумя периодами, при этом $P1(C_i) > P2(C_i)$; ‘0’ – стабильное нулевое значение, которое интерпретируется как различимая разница между двумя периодами, при этом $P1(C_i) < P2(C_i)$.

Во всем множестве полученных 128 значений $Delta(P1,P2)$ наблюдаются 8 символов «X», 62 символа «1» и 58 символов «0», что говорит о приемлемой стабильности и уникальности предложенной схемы ФНФ типа арбитр с асимметричными путями после балансировки.

Выводы

Предложен новый подход к построению физически неклонируемых функций типа арбитр, основанный на использовании заведомо несимметричных пар путей. В отличие от традиционных подходов с использованием схем мультиплексоров для переключения путей, показано, что пара независимых путей может быть спроектирована при помощи логических элементов, значениями случайных задержек которых можно управлять. Помимо этого, был предложен подход к балансировке пары независимых путей, основанный на определении типа имеющейся асимметрии. Успешно проведенные эксперименты показали состоятельность предложенного подхода, который открывает перспективы для построения новых архитектур ФНФ типа арбитр с применением различных многовходовых логических элементов, схем автобалансировки и арбитража. Дальнейшие исследования целесообразно расширить в части элементной базы: как с технологической точки зрения, так и с функциональной.

Список литературы / References

1. Pappu R. Physical *One-Way Functions*: PhD Thesis in Media Arts and Sciences. Massachusetts Institute of Technology (MIT). Cambridge, USA; 2001: 154.
2. Gassend B., Clarke D., Van Dijk M., Devadas S. Silicon Physical Random Functions. *Proc. of the 9th ACM conference on Computer and communications security*, *CCS '02*. 2002:148-160.
3. Böhm C., Hofer M. *Physical Unclonable Functions in Theory and Practice*. New York: Springer Science+Business Media; 2013: 270.
4. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонируемые функции. *Информатика*. 2011;30(2):92-103 / Yarmolik V.N., Vashinko Y.G. [Physical unclonable functions]. *Informatika = Informatics*. 2011;30(2):92-103. (In Russ.)
5. McGrath T., Bagci I.T., Wang Z.M., Roedig U., Yang R.J. A PUF taxonomy. *Applied Physics Reviews.* 2019; 6(1). DOI: https://doi.org/10.1063/1.5079407.
6. Иванюк А.А., Заливако С.С. Физическая криптография и защита цифровых устройств. *Доклады БГУИР*. 2019;(2):50-58 / Ivaniuk A.A., Zalivaka S.S. [Physical cryptography and security of digital devices]. *Doklady BGUIR = Doklady BGUIR*. 2019;(2):50-58. (In Russ.)
7. Herder C., Yu M., Koushanfar F., Devadas S. Physical Unclonable Functions and Applications: A Tutorial. *Proceedings of the IEEE*. 2014;102(8):1126-1141. DOI: 10.1109/JPROC.2014.2320516.
8. Gummalla S. *An Analytical Approach to Efficient Circuit Variability Analysis in Scaled CMOS Design: Master Degree Thesis*. Arizona: Arizona State University; 2011.

Вклад авторов

Ярмолик В.Н. предложил подход к построению физически неклонируемых функций с заведомо несимметричными путями.

Иванюк А. А. принял участие в обобщении результатов и проведении экспериментов.

Authors' contribution

Yarmolik V.N. formulated the idea of constructing physical unclonable functions with obviously asymmetric paths.

Ivaniuk A.A. took part in the generalization of the results and conduct of experiment.

Сведения об авторах

Ярмолик В.Н., д.т.н., профессор Белорусского государственного университета информатики и радиоэлектроники.

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

Information about the authors

Yarmolik V.N., Dr. of Sci. (Tech.), Professor at the Belarusian State University of Informatics and Radioelectronics.

Ivaniuk A.A., Dr. of Sci. (Tech.), Associate Professor, Professor at the Computer Science Department, Head of the Joint Educational Laboratory "SK hynix memory solutions Eastern Europe", 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. +375-29-769-96-77;
e-mail: yarmolik10ru@yahoo.com
Ярмолик Вячеслав Николаевич

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka St., 6,
Belarusian State University
of Informatics and Radioelectronics;
tel. +375-29-769-96-77;
e-mail: yarmolik10ru@yahoo.com
Yarmolik Vyacheslav Nikolaevich