УДК 004.832.32
https://doi.org/10.37661/1816-0301-2021-19-1-32-49

Оригинальная статья
Original Paper

Физически неклонируемые функции с управляемой задержкой распространения сигналов

В. Н. Ярмолик✉, А. А. Иванюк, Н. Н. Шинкевич

Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, Минск, 220013, Беларусь
✉*E-mail: yarmolik10ru@yahoo.com*

Аннотация

Цели. Решается задача построения нового класса физически неклонируемых функций (ФНФ), обеспечивающих управление задержкой распространения сигнала через элементы, которые расположены на пути его распространения. Актуальность такого исследования связана с активным развитием физической криптографии. В работе преследуются следующие цели: построение базовых элементов ФНФ и их модификаций, разработка методики построения управляемых кольцевых осцилляторов на базе элементов XOR и управляемых кольцевых осцилляторов, основанных на многовходовом переключении сигнала.

Методы. Используются методы синтеза и анализа цифровых устройств, в том числе на программируемых логических интегральных схемах, основы булевой алгебры и схемотехники.

Результаты. Показано, что комбинированные ФНФ, основанные на RS-триггерах, реализуют идею управления задержкой сигнала за счет выбора пути, который представляет собой последовательно подключенные элементы, выбранные в соответствии с запросом ФНФ. Разработана методика построения ФНФ с управляемой задержкой через каждый элемент пути. Исследованы особенности и свойства ФНФ с управляемой задержкой сигналов типа кольцевого осциллятора и показаны возможные решения для случая двухразрядных входных запросов. Предложен базовый элемент и его модификации для построения новых структур ФНФ, основанных на управлении задержкой распространения сигнала. Показано, что задержка сигнала через базовый элемент, представляющий собой многовходовый элемент XOR, зависит не только от количества входов, на которые подается активный входной сигнал, но и от фиксированного значения 0 либо 1 на остальных его входах. Приведена новая структура ФНФ – управляемый кольцевой осциллятор, рассматриваются его реализации для случая управления за счет задания количества входов, на которых изменяется активный входной сигнал.

Заключение. Предложенный подход к построению физически неклонируемых функций, основанный на управлении задержкой сигналов через логические элементы, показал свою работоспособность и перспективность. Экспериментально подтвержден эффект влияния на задержки распространения сигналов через логический элемент количества его входов, на которых изменяются входные сигналы, приводящие к изменению выходного сигнала. Перспективным представляется дальнейшее развитие идей построения управляемых кольцевых осцилляторов и осцилляторов с многовходовым переключением сигнала, а также создания новых структур ФНФ типа арбитр.

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

Благодарности. Авторы выражают искреннюю благодарность резиденту Парка высоких технологий компании SK Hynix Memory Solutions Eastern Europe за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

Для цитирования. Ярмолик, В. Н. Физически неклонируемые функции с управляемой задержкой распространения сигналов / В. Н. Ярмолик, А. А. Иванюк, Н. Н. Шинкевич // Информатика. – 2022. − Т. 19, № 1. – С. 32–49. https://doi.org/10.37661/1816-0301-2022-19-1-32-49

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 17.12.2021
Подписана в печать | Accepted 05.01.2022
Опубликована | Published 29.03.2022

Physically unclonable functions with controlled propagation delay

Vyacheslav N. Yarmolik✉, Alexander A. Ivaniuk, Natallia N. Shynkevich

Belarusian State University of Informatics and Radioelectronics,
st. P. Brovki, 6, Minsk, 220013, Belarus
✉*E-mail: yarmolik10ru@yahoo.com*

Abstract

Objectives. The problem of constructing a new class of physically uncloneable functions (PUF) based on controlling the signal propagation delay through the elements lying on the path of its propagation is being solved. The relevance of this problem is associated with the active development of physical cryptography. For its implementation, the following goals are pursued: the construction of the basic elements of the PUF and their modifications, the development of a methodology for constructing controlled ring oscillators based on XOR elements and controlled ring oscillators based on multi-input signal switching.

Methods. Methods of synthesis and analysis of digital devices were used, including those based on programmable logic integrated circuits (FPGA), the basics of Boolean algebra and circuitry.

Results. It is shown that combined PUFs based on RS-flip-flops implement the idea of controlling the signal delay by choosing a path, which is a series-connected elements selected in accordance with the PUF request. A technique for constructing an PUF with a controlled delay through each element of the path has been developed as a development of the idea of controlling the signal delay along the path. The features and properties of PUF with controlled delay of signals of the ring oscillator type are investigated and possible solutions are shown for the case of two-bit input requests. A basic element and its modifications are proposed for constructing new PUF structures based on the control of the signal propagation delay. It is shown that the signal delay through the basic element, which is a multi-input XOR element, depends not only on the number of inputs to which the active input signal is applied, but also on fixed values of 0 or 1 at its other inputs. A new PUF structure is presented, namely, a controlled ring oscillator, its implementation is considered for the case of control by setting the inputs and their number, by which the active input signal changes.

Conclusion. The proposed new approach to the construction of physically uncloneable functions, based on the control of signal delay through logical elements, has shown its efficiency and promise. The effect of the influence on the delays of signal propagation through the logic element, both the number of its inputs, along which the input signals change, leading to a change in the output signal, and their composition, is experimentally confirmed. It seems promising to further developing the ideas of constructing controlled ring oscillators and oscillators with multi-input switching of input signal, as well as the creation of new PUF structures of arbiter type.

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

Acknowledgements. The authors express their sincere gratitude to the HTP resident of the "SK Hynix Memory Solutions Eastern Europe" company for the equipment provided for carrying out experiments within the framework of the joint laboratory with the Belarusian State University of Informatics and Radioelectronics.

For citation. Yarmolik V. N., Ivaniuk A. A., Shynkevich N. N. *Physically unclonable functions with controlled propagation delay.* Informatika [*Informatics*], 2022, vol. 19, no. 1, pp. 32−49 (In Russ.). https://doi.org/10.37661/1816-0301-2022-19-1-32-49

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

Введение. Понятие *физически неклонируемых функций* было сформулировано R. Pappu в 2001 г. в работе [1], где была впервые определена концепция физических однонаправленных функций (Physical One-Way Functions). Практически одновременно B. Gassend и др. предложили реализацию кремниевых *физических случайных функций* (Physical Random Functions) [2]. Данные термины были сформулированы исторически первыми, однако в настоящее время в основном употребляется понятие «физически неклонируемые функции» (от англ. Physical Unclonable Functions, PUF). До сих пор отсутствует однозначное определение ФНФ. На практике одним из широко используемых является предложенное U. Rührmair с соавторами определение, согласно которому ФНФ представляют собой физические системы (устройства), обладающие неотъемлемым свойством неклонируемости некоторых их характеристик либо, чаще всего, параметров [3].

Основополагающее свойство неклонируемости ФНФ подразумевает, что в результате производственного процесса не получается создать два идентичных физических устройства, обладающих одинаковыми характеристиками. Изменения возникают из-за несовершенства производственного процесса и варьируются от изготовителя к изготовителю. Вместе с тем внутренние вариации физических устройств предопределены и ограничены фундаментальной физикой материалов. Они присущи структуре цифровых устройств и считаются одним из основных узких мест при тиражировании базовых элементов таких изделий. Собственные вариации цифровых устройств в целом обусловлены случайными колебаниями различного рода примесей используемых материалов, шероховатостью (неравномерностью) кромок линий соединений и компонентов (транзисторов, сопротивлений) элементов, колебаниями толщины оксида и другими причинами, где влияние со стороны изготовителя затруднено либо вообще невозможно. Эти источники вариаций вызывают изменения в значениях параметров элементов устройства и его временных задержек [4–6]. Такое влияние продолжает расти с уменьшением размера элементов цифровых устройств и в связи с изменениями технологических норм (табл. 1) [7].

Таблица 1
Математическое ожидание задержки μ инвертора и его относительная девиация σ/μ в зависимости от технологических норм

Table 1
Delay mean μ *of the inverter and its deviation* σ/μ *with respect to* μ *depending on technological nodes*

Технология, нм *Technology, nm*	Значение задержки (μ), пс *Delay mean* (μ)*, ps*	Сигма (σ/μ), % *Sigma* (σ/μ)*, %*
12	1,7	21
16	1,8	13
22	2,35	7
32	2,75	1,6
45	3,15	1,4

Данные табл. 1 показывают динамику изменения номинальной задержки μ инвертора, изготовленного по КМОП-технологии, и вариации задержки с изменением технологических норм (масштабированием). Задержки указаны в пикосекундах (пс), а технологические нормы в нанометрах (нм). Сигма (σ) представляет собой среднеквадратическое отклонение задержки. Величина σ/μ оценивает отклонение задержки сигнала от средней величины в процентах. Как видно из табл. 1, задержка уменьшается с увеличением масштабирования (уменьшением технологических норм), но ее отклонение в процентах от среднего быстро растет из-за увеличения влияния различных факторов, которые носят случайную природу. Это означает, что масштабирование

технологии обеспечивает увеличение быстродействия, но из-за роста разбросов параметров и в первую очередь задержек элементов снижает надежность как самих элементов, так и цифровых устройств на их основе.

Увеличение разбросов величин случайных значений задержки сигнала через логический элемент свидетельствует об увеличении ее непредсказуемости. Уникальность задержек и их изменяемость от элемента к элементу являются основой создания множества различных типов ФНФ для цифровых схем [8–14].

В работе [8] впервые было предложено использовать различие в задержке распространения сигнала по симметричным путям для реализации ФНФ типа арбитр (Arbiter PUF). Понятие «путь цифрового устройства» означает последовательное подключение друг к другу логических элементов, каждый из которых характеризуется задержкой распространения сигнала через элемент. В качестве альтернативы ФНФ типа арбитр в работе [9] изучено применение двух раздельных множеств путей, когда первый путь пары выбирается из первого множества элементов, а второй путь – из второго множества. Предложенная схема использует вариации задержек буфера с тремя состояниями и строится путем последовательного подключения пар буферов [9]. Разность частот кольцевых осцилляторов (Ring Oscillator PUF) [2], а также уникальность значений частот (Bistable Ring PUF) [10] были использованы в качестве основы для генерирования пар «запрос – ответ». Много реализаций ФНФ основано на применении состояния элементов памяти после инициализации на базе статического оперативного запоминающего устройства [11] и динамической памяти с произвольным доступом [12]. Рассматривались также другие подходы для создания ФНФ [13, 14], однако методологической основой большинства из них для случая интегральных цифровых схем является создание цифрового устройства, выходное значение которого определяется случайными значениями временных параметров (задержек) сигналов кремниевой подложки. Благодаря технологическим вариациям изготовления цифровых устройств время задержки сигналов по определенному пути (элементу) цифрового устройства будет незначительно отличаться от цифрового устройства к цифровому устройству и от кристалла к кристаллу, несмотря на идентичность их функциональности и топологии.

Все известные решения при создании ФНФ основаны на парадигме, согласно которой задержка по конкретному пути (элементу) имеет случайное, но неизменное и неуправляемое значение, за исключением влияния внешних факторов (температуры, давления, электромагнитного излучения и др.) и временной деградации. Это справедливо только для одновходовых элементов типа инвертора и повторителя, а также для путей, состоящих из последовательно подключенных инверторов и повторителей. Для всех остальных логических элементов с количеством входов не менее двух задержка через элемент отличается для различных входов так же, как и для разных режимов изменения входных его значений. Более того, на уровне элемента оказывается возможным управлять задержкой прохождения сигнала. Задержки через элемент принимают случайные, но в то же время неизменные значения из ограниченного множества при допущении отсутствия влияния внешних факторов и изменения их параметров с течением времени.

В настоящей статье решается задача построения нового класса ФНФ, основанного на управлении задержкой распространения сигнала через элементы, которые лежат на пути его распространения. Базовый элемент ФНФ обеспечивает управляемость задержкой за счет выбора количества входов, влияющих на изменение выходного сигнала, и значений на неактивных входах. Используя базовые элементы и их модификации, предлагаются методики построения управляемого кольцевого осциллятора на элементах XOR и управляемых кольцевых осцилляторов с функцией многовходового переключения сигнала.

Задержки 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 (среднее значение задержки) для каждого логического элемента определяется типом ис-

пользованных в них электронных элементов (например, ТТЛ, ЭСЛ, КМОП), принципиальной схемой логического элемента, технологическими нормами и особенностями процесса его изготовления.

Большинство работ по ФНФ основано на том, что изначально принимается гипотеза о фиксированном значении задержки через элемент без учета многих факторов (см., например, [4]). Эта задержка в процессе изготовления логического элемента принимает случайное значение, которое остается неизменным при функционировании ФНФ. На задержки влияют только внешние и временные факторы, они же рассматриваются разработчиками ФНФ как нежелательные эффекты.

Результатом изготовления простейшего логического элемента наподобие повторителя или инвертора будут являться два произвольных возможных значения задержек. Существует сложная и неоднозначная зависимость между этими двумя переменными, требующая глубокого и детального анализа и понимания на уровне физики процессов функционирования логического элемента. Задержки сигнала определяются на уровне 50 % размаха входного и выходного сигналов (Input and Output Signal) и обозначаются при переходе выходного сигнала из низкого уровня в высокий как Δ_{LH}, а при переходе из высокого уровня в низкий – как Δ_{HL} (рис. 1) [15].

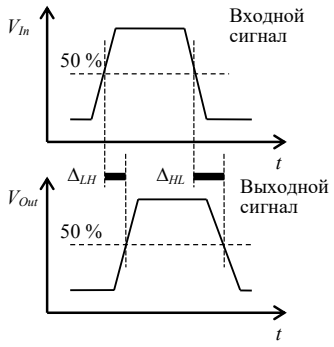


Рис. 1. Задержки Δ_{LH} и Δ_{HL} фронтов выходного импульсного сигнала

Fig. 1. Delays Δ_{LH} and Δ_{HL} of the edges of output pulse signal

Изображенные на рис. 1 временные диаграммы показывают эффект задержки сигнала через повторитель. Значения задержек фронтов (переходов) логического сигнала из 0 в 1 (Low to High, *LH*) либо из 1 в 0 (High to Low, *HL*), как правило, отличаются и в сильной степени зависят от типа электронных элементов, используемых для их изготовления. Например, времена указанных задержек сигнала при переключении КМОП-инвертора можно оценить соотношениями [15]

$$\Delta_{HL} \approx 0{,}7 \cdot R_n \cdot (C_{Oup} + C_{Load}), \quad \Delta_{LH} \approx 0{,}7 \cdot R_p \cdot (C_{Oup} + C_{Load}), \tag{1}$$

где C_{Oup} – эффективная выходная емкость инвертора, а C_{Load} – нагрузочная емкость инвертора, R_n – эффективное сопротивление *n*-канального, а R_p – *p*-канального МОП-транзистора. Разные значения эффективных сопротивлений R_n и R_p свидетельствуют об отличии времен задержек Δ_{LH} и Δ_{HL} инвертора, а технологические девиации при изготовлении МОП-транзисторов ведут к возникновению задержек с произвольными значениями в пределах своего временного интервала.

В справочной литературе для каждого логического элемента в основном приводятся средние (типовые) и (или) максимальные значения задержек Δ_{LH} и Δ_{HL} [16]. Так, для микросхемы К155ЛН1, содержащей шесть инверторов ТТЛ серии К155, указываются максимальное значение $\Delta_{LH} = 15$ нс и максимальное значение $\Delta_{HL} = 22$ нс [16].

Обобщая значения задержек Δ_{LH} и Δ_{HL} для произвольного логического элемента, определяется средняя их величина $\Delta_G = (\Delta_{LH} + \Delta_{HL})/2$, которая интерпретируется как время распространения сигнала через элемент и используется при анализе и синтезе ФНФ. В большинстве рассуж-

дений о случайности величины задержки через элемент либо путь, созданный последовательным подключением элементов, авторы оперируют задержкой Δ_G.

Как уже отмечалось, случайное значение задержки логического элемента зависит от многих факторов. Вместе с тем для конкретной принципиальной схемы элемента и специфики его изготовления у производителя задержки сигналов всегда можно описать стандартными математическими моделями, например законом распределения и численными характеристиками. Весьма важным является то, какие задержки наиболее значимы для целей построения ФНФ.

Рассмотрим задержки сигналов как источники случайности и непредсказуемости на примере простейших логических элементов. Задержки на логических элементах чаще всего исследуются в режиме переключения сигнала по одному входу элемента (Single Input Switching, SIS), изменения которого приводят к изменению выходного значения [15–17].

В работе [7] была изучена зависимость временной задержки от входа, на который подается сигнал, вызывающий изменение на выходе, для элементов, изготовленных по КМОП-технологии. Все факторы, влияющие на задержку (геометрия транзисторов, емкость нагрузки (C_{Load}), скорость нарастания входного сигнала и др.), учитываются в предложенной модели. В случае элемента 2И-НЕ с двумя входами *In*1 и *In*2 как результаты моделирования, так и аналитические расчеты показывают заметное отличие задержек в зависимости от входа, на который подается активный сигнал (табл. 2).

Таблица 2
Вариации математического ожидания задержки μ,
среднеквадратического отклонения σ и его относительная девиация σ/μ
в зависимости от активного входа элемента 2И-НЕ

Table 2
Variations in the mean μ *of the delay, the standard deviation* σ
and its relative deviation σ/μ *depending on active input of the 2NAND gate*

Вход *Input*	Результаты моделирования *Simulation results*			Аналитические результаты *Analytical results*		
	μ, пс	σ, пс	σ/μ, %	μ, пс	σ, пс	σ/μ, %
*In*1	15,60	1,68	10,77	13,86	1,17	8,43
*In*2	16,50	0,91	5,52	16,14	0,97	6,01

Более сложные процессы и, соответственно, зависимости задержек через элемент возникают в случае переключения сигналов одновременно на нескольких входах (Multi Input Switching, MIS) [15, 18]. Это происходит, например, при одновременном переключении сигналов из 1 в 0 и из 0 в 1 на обоих входах *In*1 и *In*2 элемента 2И-НЕ.

В качестве примера можно привести *m*-входовый логический элемент И-НЕ, изготовленный по КМОП-технологии. При нагрузочной емкости C_{Load} задержка Δ_{LH} распространения сигнала через элемент И-НЕ с *m* входами оценивается следующими выражениями [15]:

$$\Delta_{LH} \approx 0,7 \cdot \frac{R_p}{m} \cdot (m \cdot C_{Out} + C_{Load}),$$
$$\Delta_{LH} \approx 0,7 \cdot R_p \cdot (m \cdot C_{Out} + C_{Load}). \quad (2)$$

Здесь первое соотношение для Δ_{LH} приведено для случая переключения всех *m* входов элемента И-НЕ одновременно, а второе – только одного входа. Видно, что при переключении логического значения только на одном входе значение задержки Δ_{LH} в *m* раз больше по сравнению со случаем переключения на всех *m* входах [15].

В общем случае задержка сигнала при прохождении через логический элемент зависит от трех аргументов: пути прохождения сигнала, определяемого активным входом (входами); логических значений на неактивных входах (входе) и самих входных сигналов; задержки изменения выходного сигнала из 0 на 1 (*LH*) либо из 1 на 0 (*HL*). Подчеркнем, что временные задержки связаны с задержками переключения входного сигнала на противоположное значение, вызывающее изменение выходного сигнала. В справочной литературе обычно ука-

зываются значения оценок величин Δ_{LH} и Δ_{HL} либо их среднее значение Δ_G. Для серии К155 элементной базы ТТЛ справочными значениями для двухвходовых элементов 2XOR микросхемы К155ЛП5 являются только максимальные значения Δ_{LH} = 30 нс и Δ_{HL} = 22 нс [16].

На примере простейшего двухвходового элемента 2XOR с входами *In*1, *In*2 и выходом *Out* показано многообразие задержек прохождения сигнала, которые в процессе изготовления принимают непредсказуемые случайные значения и могут быть использованы при построении ФНФ (табл. 3).

Таблица 3
Задержки сигнала на элементе 2XOR

Table 3
Signal delays on 2XOR element

Задержка *Delay*	*In*1	*In*2	*Out*	Задержка *Delay*	*In*1	*In*2	*Out*
$\Delta_1(LH)$	*LH*	0	*LH*	$\Delta_5(HL)$	*HL*	0	*HL*
$\Delta_2(HL)$	*LH*	1	*HL*	$\Delta_6(LH)$	*HL*	1	*LH*
$\Delta_3(LH)$	0	*LH*	*LH*	$\Delta_7(HL)$	0	*HL*	*HL*
$\Delta_4(HL)$	1	*LH*	*HL*	$\Delta_8(LH)$	1	*HL*	*LH*

В табл. 3 приведены описания задержек сигнала на элементе 2XOR в режиме SIS. Например, $\Delta_2(HL)$ представляет собой задержку изменения сигнала из 1 в 0 (*HL*) на выходе *Out* при изменении входного сигнала *In*1 из 0 в 1 (*LH*) при удержании на втором входе *In*2 логической единицы. Таким образом, даже в случае простейшего двухвходового элемента XOR можно получить восемь случайных значений задержек выходного сигнала *Out*. Эти задержки зависимы между собой, так как формируются под влиянием общих факторов, присущих данному логическому элементу и его принципиальной схеме, и материалов, примененных для его реализации. Однако на каждую конкретную задержку из восьми значений, присущих элементу 2XOR, оказывают влияние различные случайные факторы в разной комбинации и в разной степени, как это следует, например, из приведенного ранее выражения (1).

Использование элементов с большим числом входов позволяет существенно расширить множество задержек, принимающих случайные значения, в первую очередь за счет режима MIS, когда одновременно изменяются значения на нескольких входах. Элемент 3И в режиме MIS при одновременном переключении сигнала формирует две задержки на трех его входах и шесть задержек на двух входах. Элемент XOR с тремя входами генерирует 24 случайные задержки в режиме SIS и 8 случайных задержек в режиме MIS при переключении значений на всех трех входах, т. е. всего 32 различающихся значения задержек выходного сигнала. Это объясняется спецификой элемента XOR, у которого изменение выходного сигнала возможно только при изменении четности значений на его входах.

Отметим, что каждая из указанных величин задержки может быть использована при построении ФНФ типа арбитр, а их многообразие позволяет управлять задержками – выбирать одну задержку из восьми (табл. 3).

Таким образом, для построения ФНФ с управляемыми задержками распространения сигнала первоначально необходима разработка базовых элементов, которые реализуют функцию управления задержкой, заключающуюся в выборе одного из возможных значений задержки.

Базовый элемент физически неклонируемых функций. Альтернативой построения ФНФ является создание автономных булевых сетей (АБС) [19, 20]. При проектировании АБС выдвигаются условия, противоположные условиям для ФНФ, а при их создании обеспечивается максимально возможная изменчивость и непредсказуемость выходных значений. Повторение измерений для АБС приводит к другим неповторяющимся выходным значениям. В ФНФ повторяемость выходных значений, называемых ответами (Responses, *R*), для одних и тех же значений запроса (Challenge, *C*) обязательна и является неотъемлемым их свойством [1, 8−14]. Вместе с тем основой непредсказуемого поведения АБС так же, как и в случае ФНФ, являются внутренние случайные вариации параметров элементов и их сочетания. Большинство решений

для получения хаотического поведения таких устройств состоит в использовании путей задержки в АБС [19, 20]. Составные компоненты АБС выполняют асимметричные логические операции, для построения которых применяются комбинации элементов логического исключающего ИЛИ (XOR) и исключающего ИЛИ с отрицанием (XNOR) [19]. Элементы XOR и XNOR имеют несколько входов, для каждого из которых искусственно (путем подключения цепочки последовательно соединенных инверторов) обеспечивается различие временных задержек.

Как и в случае с АБС, в качестве основного базового элемента для построения ФНФ используем многовходовый элемент XOR. На рис. 2, *a* изображена обобщенная структура базового элемента, обеспечивающего режим переключения своего выходного значения *Out* при прохождении входного сигнала одновременно по нескольким входам XOR. Элемент XOR базового элемента имеет $m + 1$ вход. На первый вход (*In*) элемента XOR подается входной единичный импульс, при отсутствии входного импульсного сигнала выходное значение *Out* равняется нулю.

Запрос C формируется на входах базового элемента, в качестве которого применяется m-разрядный двоичный вектор $C = c_0\, c_1 \ldots c_{m-1}$, где $c_j \in \{0, 1\}, j \in \{0, 1, \ldots, m-1\}$. В зависимости от данного запроса базовый элемент реализует один из режимов MIS. Количество ненулевых значений c_j запроса C определяет число входов XOR, через которые проходит входной импульс. Отметим, что количество единичных значений c_j для базового элемента, использующего XOR, должно быть четным, что в два раза уменьшает количество возможных значений запроса C.

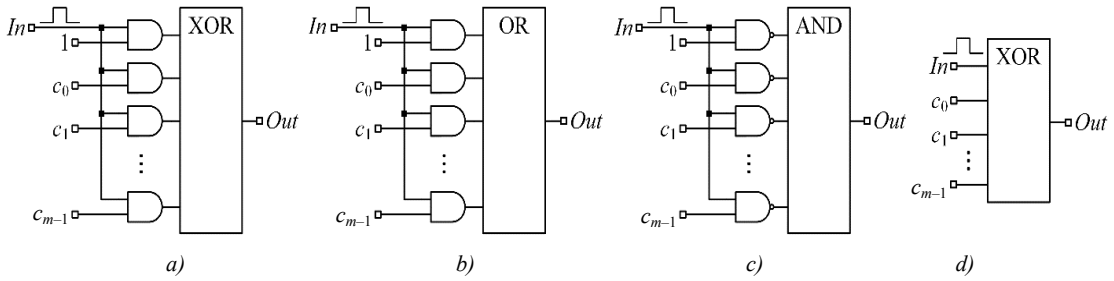


Рис. 2. Базовый элемент: *a)* структура; *b)* и *c)* модификации; *d)* режим прямого управления задержкой

Fig. 2. Basic element: a) structure; b) and c) modification; d) mode of direct control of the delay

Модификации базового элемента, использующие элементы ИЛИ (OR) и И (AND) (рис. 2, *b* и *c*), не накладывают данного ограничения на значения запроса C. В этих случаях вектор значений запроса $C = c_0\, c_1 \ldots c_{m-1}$ может принимать одно из 2^m возможных значений.

Основная идея предлагаемых в настоящей статье решений заключается в том, что для каждого запроса C базовый элемент будет иметь свое уникальное значение задержки прохождения входного импульса, определяемого режимом MIS, который задается значением вектора запроса $C = c_0\, c_1 \ldots c_{m-1}$.

Уникальность элемента XOR позволяет напрямую управлять задержкой прохождения через него входного импульса путем задания произвольных входных значений по остальным его входам (рис. 2, *d*). В данном случае выходное значение изменяется на противоположное в режиме SIS, а уникальность запроса C определяет уникальное значение задержки сигнала через элемент XOR.

Комбинированные физически неклонируемые функции. Как отмечалось ранее [11–13], статические оперативные запоминающие устройства (СОЗУ) широко используются для реализации ФНФ. Запоминающий элемент СОЗУ (ячейка) всегда находится в одном из двух состояний, что, в свою очередь, позволяет использовать его для хранения одного бита информации. Примером такой ячейки может служить RS-триггер, реализованный на двух логических элементах 2И-НЕ (рис. 3, *a*) [13].

Схема RS-триггера построена таким образом, что позволяет комбинационной схеме с положительной обратной связью хранить требуемое значение (0 или 1). Функционирование подобной схемы может быть описано с помощью таблицы переходов, однозначно определяющей функционирование RS-триггера.

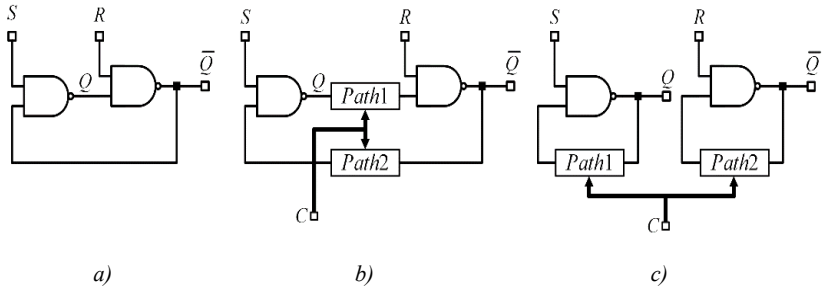


Рис. 3. Схема RS-триггера (*a*), комбинированные ФНФ (*b* и *c*)
Fig. 3. RS-flip-flop circuit (*a*)*, combined PUF* (*b and c*)

Входные значения S и R могут принимать любую из четырех возможных комбинаций: 0 0, 0 1, 1 0 или 1 1 [13]. Для обозначения безразличного значения входных сигналов S и R используется набор $X\,X \in \{0\,0, 0\,1, 1\,0, 1\,1\}$, а для выходных значений – набор $Q\ \overline{Q} \in \{0\,1, 1\,0, 1\,1\}$. Отметим, что для RS-триггера (рис. 3, *a*) на выходах Q и $\overline{Q}$ получение комбинаций $Q = 0$ и $\overline{Q} = 0$ невозможно в статическом режиме функционирования.

Высокий уровень (соответствующий логической единице) подаваемого одновременно на входы S и R RS-триггера сигнала позволяет сохранять предыдущее состояние Q, равное 0 либо 1 и определяемое последней операцией записи в данную запоминающую ячейку. Эксперименты показывают, что при включении питающего напряжения все ячейки СОЗУ устанавливаются в одно из двух возможных состояний: $Q = 0$ либо $Q = 1$. В силу симметрии RS-триггера, реализующего ячейку СОЗУ, неизвестно, какое конечное состояние Q примет ячейка: 0 или 1 [13]. В общем случае это состояние является случайным и определяется множеством факторов [11]. Эмуляцией включения питания в случае RS-триггера является последовательная подача на его входы S и R комбинаций 0 0 и 1 1 (табл. 4).

Таблица 4
Таблица переходов RS-триггера
Table 4
RS-trigger transition table

Текущие значения на входах S и R *Current values at inputs S and R*	Следующие значения на входах S и R *Next values at inputs S and R*	Текущее состояние $Q\ \overline{Q}$ *Current values* $Q\ \overline{Q}$	Следующее состояние $Q\ \overline{Q}$ *Next values* $Q\,\overline{Q}$
$S\,R = X\,X$	0 0	$Q\ \overline{Q}$	1 1
$S\,R = X\,X$	0 1	$Q\ \overline{Q}$	1 0
$S\,R = X\,X$	1 0	$Q\ \overline{Q}$	0 1
$S\,R \neq 0\,0$	1 1	$Q\ \overline{Q}$	$Q\ \overline{Q}$
$S\,R = 0\,0$	1 1	1 1	Случайное состояние Q: $\overline{Q} = 0\,1$ или $1\,0$

Большинство ячеек СОЗУ при включении питающего напряжения преимущественно переходят в одно из двух возможных состояний, поскольку каждая ячейка, представляющая собой RS-триггер, в силу специфики технологии ее изготовления имеет множество несимметричных элементов и параметров. Это в первую очередь касается длин соединительных проводников, их геометрических размеров, неоднородностей физического состава кремния, его химических свойств и, как результат, различия задержек сигналов.

Для увеличения диапазона изменения случайных значений задержек и, соответственно, стабильности и надежности ФНФ была предложена комбинированная реализация ФНФ [13]. Одним из вариантов подобных ФНФ является объединение ФНФ типа арбитр и ФНФ на базе RS-триггера. Основная идея предложенной схемы – это увеличение пути между выходом одного из двух элементов 2И-НЕ RS-триггера и входом другого элемента 2И-НЕ (см. рис. 3, *б*). Длина пути для двух обратных связей *Path*1 и *Path*2 увеличивается за счет последовательно включенных двухвходовых мультиплексоров ФНФ типа арбитр. Их количество всегда одинаково, а состав перераспределяется между двумя путями. При такой реализации задержки зависят не только от технологических вариаций во время производства логических элементов 2И-НЕ RS-триггера и их задержек, но и от значения запроса *C*. Значение формируемого запроса *C* определяет множество мультиплексоров, вариации задержек которых и влияют на значение ответа.

Необходимо отметить, что запрос *C* определяет не только значение задержек по двум путям *Path*1 и *Path*2, но и структуру комбинированного генератора [13]. При четном количестве единичных значений в векторе запроса $C = c_0\, c_1 \ldots c_{m-1}$ реализуется комбинация ФНФ типа арбитр и ФНФ на базе RS-триггера. Если число единичных значений в запросе нечетное, то в этом случае получим комбинацию ФНФ типа арбитр и кольцевого осциллятора (RO) (см. рис. 3, *c*) [13]. Отличием двух структур комбинированных ФНФ является режим их функционирования, который в первом случае повторяет функционирование ФНФ на базе RS-триггера, а во втором − функционирование кольцевого осциллятора.

В то же время общим для обоих вариантов комбинированных ФНФ является задание значений задержек по цепям обратной связи RS-триггера (см. рис. 3, *b*) и задержек работы двух кольцевых осцилляторов (см. рис. 3, *c*). Значения величин задержек в указанных структурах ФНФ определяются задержками мультиплексоров, возникающими в результате генерирования конкретного запроса *C*. Для каждого нового запроса *C* формируются новые пути *Path*1 и *Path*2, состоящие из других комбинаций тех же мультиплексоров, каждый из которых имеет свое уникальное время задержки.

Появление комбинированных ФНФ, основанных на структурах типа арбитр, повторяет идею задания определенных задержек по двум путям, сформированным из последовательно включенных мультиплексоров. Однако при рассмотрении этих же решений (см. рис. 3, *b* и *c*) с точки зрения ФНФ на базе RS-триггера и RO ФНФ можно сделать совершенно другие выводы. Так, структура, изображенная на рис. 3, *b*, представляет собой ФНФ на базе RS-триггера с управляемыми задержками по цепям обратной связи, а на рис. 3, *c* показаны два RO ФНФ с изменяемыми (управляемыми) частотами функционирования. В обоих случаях изначально управление заключается в выборе определенных задержек сигналов в соответствии с заданным запросом *C*.

Развивая классическую идею управления задержками сигналов через множество последовательно подключенных элементов, рассмотрим ряд решений управления задержками на уровне одного элемента. В качестве основы таких решений используем базовый элемент и его модификации, представленные на рис. 2.

ФНФ с управляемыми задержками на уровне элементов. Как отмечалось ранее, все известные решения при создании ФНФ основаны на том, что задержка по конкретному пути (элементу) имеет случайное, но вместе с тем неизменное и неуправляемое значение. Изменение задержки как результат влияния внешних факторов, таких как температура, давление, электромагнитное излучение, а также деградация физических и химических свойств частей элементов, относятся к негативным и нежелательным эффектам для ФНФ.

В качестве альтернативного подхода для построения ФНФ в настоящей статье обосновывается возможность построения нового класса ФНФ с управляемыми задержками. Первоначально рассмотрим простейший случай базового элемента (см. рис. 2, *d*), представляющего собой двухвходовый элемент XOR, один из входов которого управляющий. При подаче на второй вход этого элемента изменяющегося входного значения выходное значение XOR изменяется на противоположное. Двоичное значение $c_i = 0$ либо $c_i = 1$ на управляющем входе будет определять величину задержки изменения выходного значения *i*-го двухвходового элемента XOR. Ис-

пользуя n последовательно подключенных двухвходовых сумматоров по модулю два (XOR), построим схему управляемого кольцевого осциллятора (Controlled Ring Oscillator, CRO) в упрощенном виде (рис. 4).

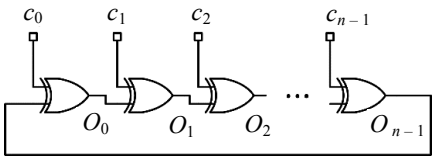


Рис. 4. Управляемый кольцевой осциллятор
Fig. 4. Controlled ring oscillator

Уникальность двухвходового элемента XOR позволяет напрямую управлять задержкой прохождения через него входного импульса путем задания произвольного входного значения 0 либо 1 по его управляющему входу. Предположив, что i-й элемент XOR имеет задержку d_{i0} при $c_i = 0$ и задержку d_{i1} при $c_i = 1$, суммарная задержка D прохождения сигнала через n последовательно подключенных элементов CRO определяется согласно соотношению

$$D = \sum_{i=0}^{n-1} (c_i d_{i1} + \overline{c}_i d_{i0}). \quad (3)$$

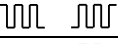
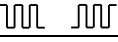
В конечном счете величина задержки D и определяет частоту $f = 1/(2D)$ генерируемых периодических сигналов управляемым кольцевым осциллятором при условии обеспечения отрицательной обратной связи. Необходимым и достаточным условием наличия такой связи является нечетное количество единичных значений c_i запроса $C = c_0\, c_1 \ldots c_{n-1}$.

Таким образом, ФНФ типа CRO, показанная на рис. 4, представляет собой 2^{n-1} классических кольцевых осциллятора RO, каждый из которых имеет свою уникальную частоту формирования выходных сигналов.

Допустив возможность задания любого из 2^m запросов C при функционировании CRO, можно заметить, что его поведение напоминает функционирование комбинированных ФНФ, рассмотренных ранее [13]. Детально исследуем поведение CRO для случая $n = 2$, когда структура, приведенная на рис. 4, представляется двумя последовательно включенными двухвходовыми элементами XOR (табл. 5).

Таблица 5
Описание функционирования CRO для случая $n = 2$

Table 5
Description of CRO *functioning for the case n = 2*

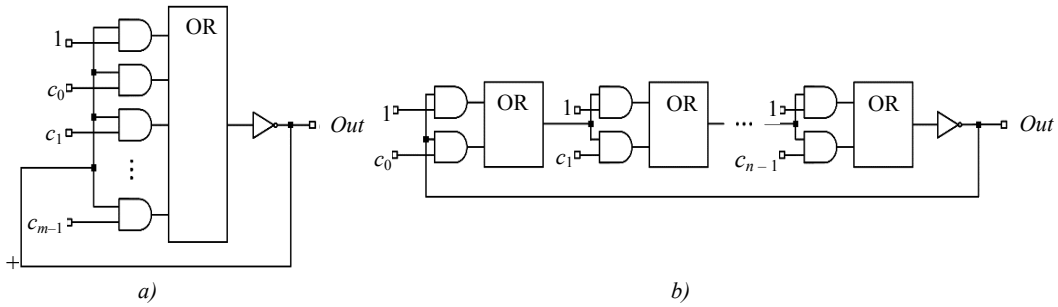
Текущие значения на входах c_0 и c_1 *Current values at inputs c_0 and c_1*	Следующие значения на входах c_0 и c_1 *Next values at inputs c_0 and c_1*	Текущее состояние $O_0\, O_1$ *Current values $O_0\, O_1$*	Следующее состояние $O_0\, O_1$ *Next values $O_0\, O_1$*
$c_0\, c_1 = 0\, 0$	0 0	$O\, O$	$O\, O$
$c_0\, c_1 = 0\, 1$ $c_0\, c_1 = 1\, 0$ $c_0\, c_1 = 1\, 1$	0 0	Любое, кроме $O\, O$	Случайное состояние $O\, O$
$c_0\, c_1 = X\, X$	0 1	Произвольное	
$c_0\, c_1 = X\, X$	1 0	Произвольное	
$c_0\, c_1 = 1\, 1$	1 1	$O\, \overline{O}$	$O\, \overline{O}$
$c_0\, c_1 = 0\, 0$ $c_0\, c_1 = 0\, 1$ $c_0\, c_1 = 1\, 0$	1 1	Любое, кроме $O\, \overline{O}$	Случайное состояние $O\, \overline{O}$

Из табл. 5 видно, что выходные значения O_0 и O_1 могут принимать и одинаковые ($O \in \{0, 1\}$), и противоположные (O и $\overline{O}$) значения. При подаче на входы c_0 и c_1 нулевых значений на выходах O_0 и O_1 формируются одинаковые значения O O, нулевые либо единичные. Аналогично функционирует CRO и в случае подачи на его входы единичных значений, при этом на выходах O_0 и O_1 формируются инверсные значения O и $\overline{O}$. В обоих случаях обеспечивается положительная обратная связь, определяющая устойчивое состояние CRO, который представляет собой комбинационную схему. Для входных значений 0 1 и 1 0 схема CRO будет генерировать высокочастотные колебания выходного сигнала, так как эти значения входных сигналов обеспечивают отрицательную обратную связь. При этом в первом случае частота сигнала определяется задержкой $d_{00} + d_{11}$, а во втором – суммарной задержкой $d_{01} + d_{10}$. В табл. 5 термин «произвольное» обозначает одно из следующих пяти возможных состояний: 0 0, 0 1, 1 0, 1 1 и состояние кольцевого генератора по выходам O_0 и O_1 CRO.

Как и для классического RS-триггера, для структуры CRO существуют ситуации неопределенного (случайного) поведения. Напомним, что формирование на входах RS-триггера значений 1 1 после входной комбинации 0 0 приводит к случайному состоянию RS-триггера (см. табл. 4). В случае CRO генерирование на входах c_0 и c_1 комбинации 0 0 после любой другой комбинации входных значений так же, как и формирование входных значений 1 1 после отличной от подаваемой ранее входной комбинации, приводит к установке CRO в произвольное (случайное) состояние (см. табл. 5).

Управляемые кольцевые осцилляторы, основанные на многовходовом переключении активного сигнала. Ранее уже отмечалось, что более сложные процессы и, соответственно, зависимости задержек через элемент возникают в случае переключения сигналов одновременно на нескольких входах (MIS) базового элемента и его модификаций, представленных на рис. 2. Под *активным сигналом* понимают значение входного сигнала элемента, изменение которого приводит к изменению выходного значения элемента. Модификации исходного базового элемента, показанные на рис. 2, *b* и *c*, позволяют управлять с помощью запроса C количеством переключающихся входных значений, которые изменяют выходное значение базового элемента. Отметим, что не только количество входов, но и их конкретный набор определяются запросом C, в результате чего и происходит задание конкретной задержки через базовый элемент.

Для построения CRO с многовходовым переключением входного сигнала (Multi Input Switching Controlled Ring Oscillator, MISCRO) исходными данными будут являться размерность n запроса C, управляющего величиной задержки, и ее математическое ожидание (среднее значение задержки). Эти два параметра для CRO, изображенного на рис. 4, находятся в полном противоречии. Рост количества 2^n возможных запросов CRO увеличивает значение n и, соответственно, среднее значение общей задержки D (3), что существенно уменьшает быстродействие CRO. Для возможности нахождения компромисса между размерностью n запроса C предлагаемых структур MISCRO и его задержками (быстродействием) приведем две его полярные реализации (рис. 5).



a) *b)*

Рис. 5. Управляемый кольцевой осциллятор с многовходовым переключением входного сигнала: *a)* первая реализация; *b)* вторая реализация

Fig. 5. Controlled ring oscillator with multi-input switching of input signal: a) first implementation; b) second implementation

Представленные на рис. 5 схемы основаны на модификации базового элемента (см. рис. 2, *b*). Первая реализация MISCRO (рис. 5, *a*) использует $m + 1$ входовый элемент ИЛИ (OR), на котором задействован режим переключения выходного значения на противоположное состояние при изменении активного сигнала более чем по одному входу. Конкретные входы и их количество определяются ненулевыми компонентами $c_i \in \{0, 1\}$ запроса $C = c_0\, c_1 \ldots c_{n-1}$. Для разных значений C задержка изменения выходного значения, как показывалось ранее, различна. За счет отрицательной обратной связи данная схема генерирует высокочастотный сигнал подобно классическому RO. Не вдаваясь в особенности реализации многовходовых логических элементов, можно констатировать, что первая схема MISCRO характеризуется максимальной частотой формируемого сигнала. Эта частота определяется суммарной задержкой только трех последовательно включенных логических элементов.

Вторая реализация MISCRO (рис. 5, *b*) имеет минимальное быстродействие в силу большого количества последовательно подключенных логических элементов, охваченных отрицательной обратной связью. По сравнению с первой реализацией (рис. 5, *a*) суммарная средняя задержка сигнала может быть больше для второй схемы практически в $(2n + 1)/(n + 2) \div (2n + 1)/3$ раз. Нижняя оценка $(2n + 1)/(n + 2)$ получена при допущении, что задержки сигналов элементов 2И, 2ИЛИ и НЕ одинаковы, а задержка n-входового элемента ИЛИ в n раз больше задержки аналогичного элемента с двумя входами. Верхняя оценка $(2n + 1)/3$ получена при тех же допущениях об одинаковых значениях задержки, но безотносительно количества входов в элементе, т. е. задержки и двухвходового, и n-входового элементов ИЛИ принимались равными. Из приведенных оценок видно, что быстродействие MISCRO, представленного на рис. 5, *a*, практически в два раза больше быстродействия MISCRO на рис. 5, *b*. Возможны компромиссные решения, когда количество входов элемента ИЛИ будет больше двух, но меньше n. Подобные решения возможны и для других модификаций базового элемента, равно как и развитие модификаций на рис. 5. Например, схема на рис. 5, *a* может быть упрощена за счет удаления элемента 2И, на второй вход которого подается значение 1, при одновременном запрете на применение запроса $C = c_0\, c_1 \ldots c_{n-1} = 0\ 0\ \ldots\ 0$.

Еще бóльшие возможности имеет предлагаемый авторами подход при построении реализующих схемы типа арбитр ФНФ, когда сравниваются задержки по двум уникальным путям, построенным за счет реконфигурации этих путей в соответствии со значением запроса C.

Экспериментальные исследования. Практические исследования были направлены на подтверждение главной идеи авторов, заключающейся в том, что простейший логический элемент является источником уникальных значений задержки прохождения входного сигнала. Уникальность и непредсказуемость величины задержки, как уже отмечалось ранее, определяется в основном технологическими нормами и особенностями процесса изготовления логического элемента. Поэтому авторы сконцентрировали свое внимание на реальных цифровых устройствах.

В ходе первого эксперимента было получено подтверждение, что элемент 2XOR является источником восьми значений задержки сигнала (см. табл. 3), каждое из которых может использоваться при построении ФНФ. Исследования проводились для интегральной схемы К155ЛП5 (URL: http://chiplist.ru/chips/K155LP5/, https://pdf1.alldatasheet.com/datasheet-pdf/view/27431/TI/SN7486N.html), которая имеет в своем составе четыре (*A*, *B*, *C* и *D*) двухвходовых элемента XOR [17]. Суть эксперимента заключалась в определении основных статистических характеристик, таких как математические ожидания задержки μ, и среднеквадратического отклонения σ для каждой из восьми задержек $\Delta_1(LH)$, $\Delta_2(HL)$, …, Δ_8(LH). Эксперименты проводились для различных экземпляров микросхемы К155ЛП5 и четырех двухвходовых элементов XOR, входящих в их состав. На один из входов двухвходового элемента XOR подавались тестовые импульсы прямоугольной формы при помощи генератора сигналов специальной формы АКИП-3409/1 (URL: https://www.electronpribor.ru/catalog/51/akip-3409_1.htm). Измерение задержек $\Delta_1(LH)$, $\Delta_2(HL)$, …, $\Delta_8(LH)$ распространения фронта тестового сигнала от входа *In*1 либо *In*2 до выхода *Out* (см. табл. 3) осуществлялось при помощи двухканального цифрового осциллографа Rohde & Schwarz RTB2002 (URL: https://www.rohde-schwarz. com/ru/product/rtb2000-productstartpage_63493-266306.html). В качестве примера в табл. 6 даны результаты экспери-

ментов для двух (*A* и *B*) элементов XOR, принадлежащих двум различным микросхемам К155ЛП5#1 и К155ЛП5#2. Каждый эксперимент состоял в проведении 50 измерений задержки с последующим определением ее статистических характеристик. Численные характеристики, приведенные в табл. 6, согласуются со справочными данными микросхемы SN7486N, являющейся аналогом микросхемы К155ЛП5 (URL: https://pdf1.alldatasheet.com/ datasheet-pdf/view/27431/TI/SN7486N.html).

Таблица 6
Статистические характеристики задержек для элементов XOR микросхем К155ЛП5#1 и К155ЛП5#2

Table 6
Statistical characteristics of time delays for elements XOR of integrated circuits K155LP5#1 and K155LP5#2

Задержка, нс *Delay, ns*	$\Delta_1(LH)$	$\Delta_2(HL)$	$\Delta_3(LH)$	$\Delta_4(HL)$	$\Delta_5(HL)$	$\Delta_6(LH)$	$\Delta_7(HL)$	$\Delta_8(LH)$
К155ЛП5#1 (A)								
μ	30,48	20,85	31,18	19,31	16,73	38,84	15,35	36,68
σ	0,240	0,109	0,146	0,270	0,266	0,108	0,303	0,269
К155ЛП5#1 (B)								
μ	36,40	23,64	33,51	28,13	17,18	37,21	16,40	38,18
σ	0,168	0,144	0,204	0,123	0,070	0,094	0,129	0,132
К155ЛП5#2 (A)								
μ	35,31	17,75	29,70	16,53	20,35	39,63	16,48	37,88
σ	0,195	0,259	0,249	0,198	0,129	0,163	0,187	0,156
К155ЛП5#2 (B)								
μ	36,05	26,20	37,72	26,70	17,87	38,06	16,69	38,50
σ	0,093	0,155	0,107	0,156	0,108	0,080	0,058	0,104

Анализ результатов, представленных в табл. 6, позволяет сделать вывод о том, что все восемь значений задержек элемента 2XOR различимы и могут быть использованы для управления задержкой через элементы CRO путем выбора одного из них. Отличие значений одной и той же задержки для двух разных (*A* и *B*) элементов XOR одной микросхемы и их различие в зависимости от анализируемой микросхемы свидетельствуют о возможности создания CRO.

Второй эксперимент был нацелен на подтверждение следующей идеи, предлагаемой авторами для схемы CRO: для каждого запроса *C* базовый элемент генератора будет иметь свое уникальное значение задержки прохождения импульса, что, в свою очередь, приведет к уникальности частоты формируемых CRO импульсных последовательностей. Для проведения эксперимента была спроектирована схема CRO (см. рис. 4) для случая $n = 8$ и реализована на программируемой логической интегральной схеме (ПЛИС) Xilinx XC7Z010-1CLG00C (URL: https://www.xilinx.com/content/dam/xilinx/support/documentation/data_sheets/ds190-Zynq-7000-Overview.pdf), входящей в состав платы быстрого прототипирования Digilent ZYBO Z7 (URL: https://digilent.com/reference/programmable-logic/zybo-z7/start). Использованная ПЛИС изготовлена по КМОП-технологии HKMG (High-K Metal Gate) с применением технологической нормы 28 нм.

Спроектированная схема CRO имеет в своем составе дополнительный логический элемент 2И, расположенный в цепи обратной связи осциллятора, для обеспечения стартстопного режима работы. Структурные элементы схемы осциллятора размещены на фиксированных элементах 2XOR (технологическом примитиве XORCY), входящих в состав конфигурируемого блока ускоренного переноса CARRY4 (Carry Chain Block; URL: https://www.xilinx.com/support/ documentation/user_guides/ug474_7Series_CLB.pdf).

Помимо самого осциллятора, были спроектированы и реализованы дополнительные схемы его управления, такие как генератор разрешающего сигнала с программируемой длительностью, 32-разрядные счетчики для подсчета числа сгенерированных импульсов и общая схема управления и передачи данных для микропроцессорной системы ARM, входящей в состав ПЛИС. Кроме этого, было реализовано встраиваемое программное обеспечение, позволя-

ющее управлять экспериментом и передавать полученные данные на рабочую станцию для дальнейшего анализа. Для проектирования и реализации аппаратно-программной системы проведения эксперимента была использована САПР Xilinx Vivado/Vitis 2021 (URL: https://www.xilinx.com/products/design-tools/vivado.html, https://www.xilinx.com/products/design-tools/vitis/vitis-platform. html).

Эксперимент заключался в подаче всех возможных конфигурационных запросов C_i, удовлетворяющих условию

$$w(C_i) = 2j - 1, \ \forall\, i \in \{0, 1, \ldots, 2^n - 1\}, \ \ j \in \{1, 2, \ldots, n/2\},$$

где w – вес Хэмминга вектора запроса C_i. Для каждого из сформированных запросов был произведен подсчет числа сгенерированных импульсов в пределах фиксированного временного окна измерения. Из полученных данных вычислялись значения периодов генерируемых сигналов на выходе кольцевого осциллятора. Значения периодов сигналов, вырабатываемых схемой CRO, в зависимости от подаваемого запроса C_i представлены на рис. 6.

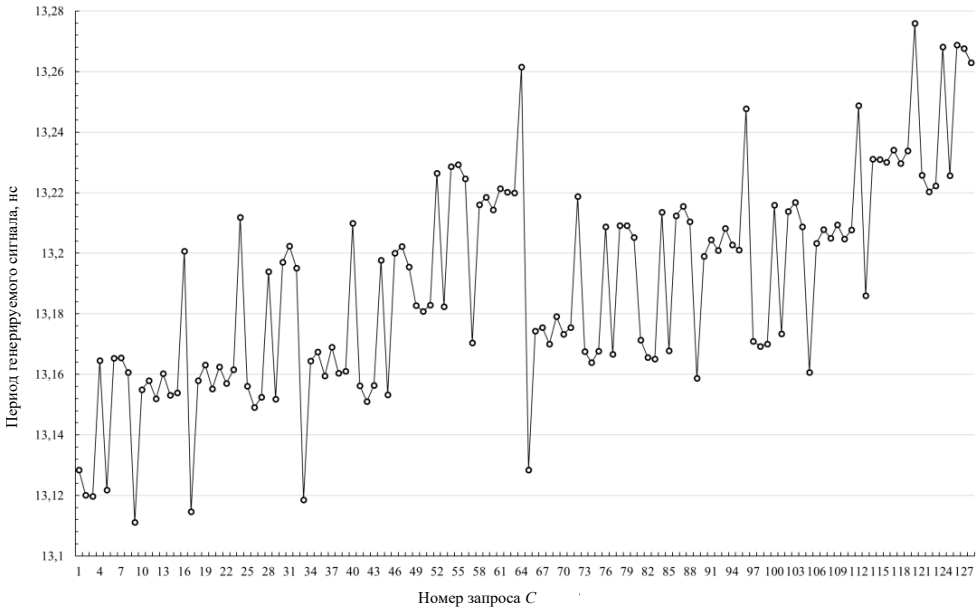


Рис. 6. Зависимость периода генерируемого сигнала от подаваемого запроса

Fig. 6. Dependence of the period of generated signal on submitted challenge

На рис. 7 показана зависимость математического ожидания периодов сигналов от значений запросов для четырех различных ПЛИС.

Согласно формуле (3) все множество уникальных запросов C формирует $2^{n-1} = 128$ уникальных значений $2D$ периодов сигналов, вырабатываемых конфигурируемым осциллятором в диапазоне [13,111; 13,276] нс. Таким образом, можно утверждать, что все структурные элементы 2XOR генератора обладают уникальными значениями задержек d_{i0} и d_{i1}.

Дополнительно были проведены 100 экспериментов, в ходе которых оценивались значения математического ожидания μ и среднеквадратического отклонения σ периодов сигналов, вырабатываемых схемой CRO, в зависимости от всех возможных значений запроса. Так, для многократно повторяемых 128 запросов в 100 экспериментах значения μ принадлежат диапазону [13,11183; 13,27604] нс, а значения σ – диапазону [0,00094; 0,00205] нс.

Для подтверждения факта уникальности эксперимент был повторен на трех других идентичных платах и ПЛИС Xilinx XC7Z010-1CLG00C. При этом использовался такой же BIT-образ конфигурации, что и в эксперименте с первой ПЛИС.

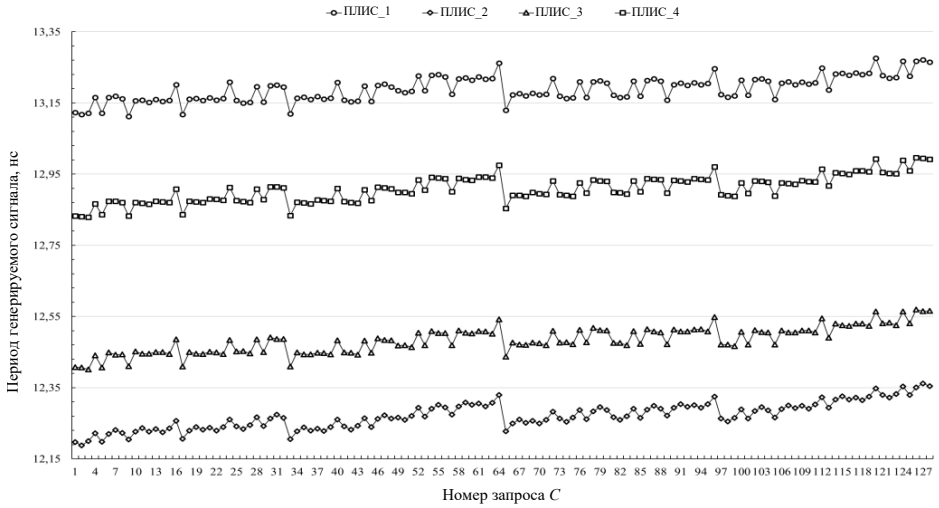


Рис. 7. Зависимость периодов генерируемых сигналов от подаваемых запросов для четырех ПЛИС

Fig. 7. Dependence of the periods of generated signal on the submitted challenges for four FPGAs

Таким образом, предположение о зависимости временных задержек от значений подаваемых запросов для схемы управляемого кольцевого генератора CRO, выдвинутое авторами, подтверждается. Можно утверждать, что временные задержки зависят от управляемых параметров (значения запроса C, протяженности n конфигурируемого пути) и неуправляемых уникальных характеристик его структурных элементов.

Заключение. Предложенный подход к построению физически неклонируемых функций, основанный на управлении задержкой сигналов через логические элементы, показал свою работоспособность и перспективность. Интересными представляются дальнейшее развитие идей построения управляемых кольцевых осцилляторов CRO и MISCRO, а также создание новых структур ФНФ типа арбитр. Дальнейшие исследования целесообразно расширить в части элементной базы как с технологической, так и функциональной точек зрения. В первую очередь необходимы уточнения особенностей управления задержкой для КМОП-технологии и практической реализации предложенных схем на различного рода программируемых структурах.

Вклад авторов. *В. Н. Ярмолик* предложил идею построения физически неклонируемых функций с управляемой задержкой сигналов. *А. А. Иванюк* принял участие в обобщении и анализе полученных результатов и проведении экспериментальных исследований. *Н. Н. Шинкевич* провела экспериментальные исследования.

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. Controlled physical random functions / B. Gassend [et al.] // Proc. of 18th Annual Computer Security Applications Conf. (ACSAC), Las Vegas, Nevada, USA, 9–13 Dec. 2002. – Las Vegas, 2002. – P. 149–160.

3. Rührmair, U. Strong PUFs: models, constructions, and security proofs / U. Rührmair, H. Busch, S. Katzenbeisser // Towards Hardware-Intrinsic Security / eds. A.-R. Sadeghi, D. Naccache. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2010. – P. 79–96.

4. Agarwal, A. Statistical timing analysis for intra-die process variations with spatial correlations / A. Agarwal, D. Blaauw, V. Zolotov // Proc. of Intern. Conf. on Computer Aided Design (ICCAD03), San Jose, CA, USA, 9–13 Nov. 2003. – San Jose, 2003. – P. 900–907.

5. Böhm, C. Physical Unclonable Functions in Theory and Practice / C. Böhm, M. Hofer. – N. Y. : Springer Science + Business Media, 2013. – 270 p.

6. Theoretical analysis of delay-based PUFs and design strategies for improvement / Y. Wang [et al.] // Proc. of the IEEE Intern. Symp. on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019. – Sapporo, 2019. – P. 1–5.

7. Gummalla, S. An Analytical Approach to Efficient Circuit Variability Analysis in Scaled CMOS Design: Master Degree Thesis / S. Gummalla. – Arizona : Arizona State University, 2011. – 62 p.

8. A technique to build a secret key in integrated circuits for identification and authentication applications / J. W. Lee [et al.] // Proc. of the Intern. Symp. VLSI Circuits (VLSI'04), Honolulu, Hawaii, USA, 7–19 June 2004. – Honolulu, 2004. – P. 176–179.

9. Ozturk, E. Physical unclonable function with tristate buffers / E. Ozturk, G. Hammouri, B. Sunar // Proc. of the IEEE Intern. Symp. on Circuits and Systems (ISCAS 2008), Seattle, Washington, USA, 18–21 May 2008. – Seattle, 2008. – P. 3194–3197.

10. The bistable ring PUF: A new architecture for strong physical unclonable functions / Q. Chen [et al.] // Proc. of the IEEE Intern. Symp. on Hardware Oriented Security and Trust (HOST'11), San Diego, California, USA, 5–6 June 2011. – San Diego, 2011. – P. 134–141.

11. Holcomb, D. E. Power-up SRAM state as an identifying fingerprint and source of true random numbers / D. E. Holcomb, W. Burleson, K. Fu // IEEE Transactions on Computer. – 2008. – Vol. 58, no. 9. – P. 1198–1210.

12. DRAM-based intrinsic physically unclonable functions for system-level security and authentication / F. Tehranipoor [et al.] // IEEE Transactions on Very Large Scale Integration (VLSI) Systems. – 2016. – No. 99. – P. 1–13.

13. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – № 2(30). – С. 92–103.

14. Иванюк, А. А. Физическая криптография и защита цифровых устройств / А. А. Иванюк, С. С. Заливако // Доклады БГУИР. – 2019. – № 2(120). – С. 50–58.

15. Верниковский, Е. А. Схемотехника: учебно-методический комплекс / Е. А. Верниковский. – Минск : БГУ, 2012. – 200 с.

16. Jouppi, N. Timing analysis and performance improvement of MOS VLSI designs / N. Jouppi // IEEE Transactions on Computer-Aided Design. – 1987. – Vol. 6, no. 4. – P. 650–665.

17. Богданович, М. И. Цифровые интегральные микросхемы / М. И. Богданович, И. Н. Грель, В. А. Прохоренко. – Минск : Беларусь, 1991. – 493 с.

18. Ram, O. V. S. S. Modeling multiple-input switching in timing analysis using machine learning / O. V. S. S. Ram, S. Saurabh // IEEE Trans. on Computer. – 2021. – Vol. 40, no. 4. – P. 723–734.

19. Experiments on autonomous Boolean networks / D. P. Rosin [et al.] // Chaos: An Interdisciplinary J. of Nonlinear Science. – 2013. – Vol. 23, no. 2. – P. 1–9.

20. Park, M. True random number generation using CMOS Boolean chaotic oscillator / M. Park, J. C. Rodgers, D. P. Lathrop // Microelectronics J. – 2015. – Vol. 46, no. 12. – P. 1364–1370.

References

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

2. Gassend B., Clarke D., Dijk M. S., Devadas S. Controlled physical random functions. *Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC), Las Vegas, Nevada, USA, 9–13 December 2002*. Las Vegas, 2002, pp. 149–160.

3. Rührmair U., Busch H., Katzenbeisser S. Strong PUFs: Models, Constructions, and Security Proofs. *Towards Hardware-Intrinsic Security*. In Sadeghi A.-R., Naccache D. (eds.). Berlin, Heidelberg, Springer Berlin Heidelberg, 2010, pp. 79–96.

4. Agarwal A., Blaauw D., Zolotov V. Statistical timing analysis for intra-die process variations with spatial correlations. *Proceedings of the International Conference on Computer Aided Design (ICCAD03), San Jose, CA, USA, 9–13 November 2003*. San Jose, 2003, pp. 900–907.

5. Böhm C., Hofer M. *Physical Unclonable Functions in Theory and Practice*. New York, Springer Science + Business Media, 2013, 270 p.

6. Wang Y., Wang C., Gu C., Cui Y. Theoretical analysis of delay-based PUFs and design strategies for improvement. *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan, 26–29 May 2019*. Sapporo, 2019, pp. 1–5.

7. Gummalla S. *An Analytical Approach to Efficient Circuit Variability Analysis in Scaled CMOS Design: Master Degree Thesis*. Arizona, Arizona State University, 2011, 62 p.

8. Lee J. W., Lim D., Gassend B., Suh G., Dijk M., Devadas S. A technique to build a secret key in integrated circuits for identification and authentication applications. *Proceedings of the International Symposium VLSI Circuits (VLSI'04), Honolulu, Hawaii, USA, 7–19 June 2004.* Honolulu, 2004, pp. 176–179.

9. Ozturk E., Hammouri, G., Sunar B. Physical unclonable function with tristate buffers. *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS 2008), Seattle, Washington, USA, 18–21 May 2008*. Seattle, 2008, pp. 3194–3197.

10. Chen Q., Csaba G., Lugli P., Schlichtmann U., Rührmair U. The bistable ring PUF: A new architecture for strong physical unclonable functions. *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST'11), San Diego, California, USA, 5–6 June 2011.* San Diego, 2011, pp. 134–141.

11. Holcomb D. E., Burleson W., Fu K. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers*, 2008, vol. 58, no. 9, pp. 1198–1210.

12. Tehranipoor F., Karimian N., Xiao K., Chandy J. DRAM-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2016, no. 99, pp. 1–13.

13. Yarmolik V. N., Vashinko Y. G. *Physical unclonable functions.* Informatika [*Informatics*], 2011, no. 2(30), pp. 92–103 (In Russ.).

14. Ivaniuk A. A., Zalivaka S. S. *Physical cryptography and security of digital devices*. Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioèlektroniki [*Reports of the Belarusian State University of Informatics and Radioelectronics*], 2019, no. 2(120), pp. 50–58 (In Russ.).

15. Vernikovskii E. A. Schemotehnika: uchebno-metodicheskii complex. *Circuitry: Educational-methodical Complex*. Minsk, Belorusskij gosudarstvennyj universitet, 2012, 200 p. (In Russ.).

16. Jouppi N. Timing analysis and performance improvement of MOS VLSI designs. *IEEE Transactions on Computer-Aided Design*, 1987, vol. 6, no. 4, pp. 650–665.

17. Bogdanovich M. I., Grel' I. N., Prohorenko V. A. Tsifrovue integral'nue mikroshemy. *Digital Integrated Circuits*, Minsk, Belarus, 1991, 493 p. (In Russ.).

18. Ram O. V. S. S., Saurabh S. Modeling multiple-input switching in timing analysis using machine learning. *IEEE Transactions on Computer*, 2021, vol. 40, no. 4, pp. 723–734.

19. Rosin D. P., Rontani D., Gauthier D. J. Experiments on autonomous Boolean networks. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 2013, vol. 23, no. 2, pp. 1–9.

20. Park M., Rodgers J. C., Lathrop D. P. True random number generation using CMOS Boolean chaotic oscillator. *Microelectronics Journal*, 2015, vol. 46, no. 12, pp. 1364–1370.

Информация об авторах

Ярмолик Вячеслав Николаевич, доктор технических наук, профессор, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: yarmolik10ru@yahoo.com

Иванюк Александр Александрович, доктор технических наук, доцент, профессор кафедры информатика и заведующий совместной учебной лабораторией SK Hynix Memory Solutions Eastern Europe, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: ivaniuk@bsuir.by

Шинкевич Наталья Николаевна, аспирант, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: nn5h@yahoo.com

Information about the authors

Vyacheslav N. Yarmolik, D. Sc. (Eng.), Professor, Belarusian State University of Informatics and Radioelectronics.
E-mail: yarmolik10ru@yahoo.com

Alexander A. Ivaniuk, D. Sc. (Eng.), Assoc. Prof., Professor of Comp. Sci. Department, Head of the Joint Educational Laboratory "SK Hynix Memory Solutions Eastern Europe", Belarusian State University of Informatics and Radioelectronics.
E-mail: ivaniuk@bsuir.by

Natallia N. Shynkevich, Graduate Student, Belarusian State University of Informatics and Radioelectronics.
E-mail: nn5h@yahoo.com