УДК: 004.312

Александр А. Иванюк[1], Вячеслав Н. Ярмолик[2]
Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, Минск, 220013, Беларусь
[1]e-mail: ivaniuk@bsuir.by, https://orcid.org/0000-0002-6541-7742
[2]e-mail: yarmolik10ru@yahoo.com, https://orcid.org/0000-0003-3995-1463

ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ НА БАЗЕ УПРАВЛЯЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

DOI: http://dx.doi.org/10.26583/bit.2023.3.06

Аннотация. Решается задача построения нового класса физически неклонируемых функций (ФНФ) на базе управляемого кольцевого осциллятора (УКО). Актуальность создания УКОФНФ связана с активным развитием физической криптографии, применяемой для целей идентификации электронных изделий и формирования криптографических ключей. Показано, что классические физически неклонируемые функции на основе кольцевых осцилляторов (КОФНФ) характеризуются большой аппаратурной избыточностью из-за необходимости реализовывать большое число КО, в силу того что, каждый бит ответа требует наличия независимой пары реальных КО. В тоже время КОФНФ характеризуются лучшими статистическими свойствами по сравнению с ФНФ типа арбитр и не требуют обеспечения идеальной симметричности и идентичности реализуемых КО. В качестве альтернативы КОФНФ предлагается новый класс физически неклонируемых функций, а именно УКОФНФ, использующий управляемые кольцевые осцилляторы, основанные на управлении частотой формируемых импульсов без изменения функциональности и структуры осциллятора. Важным достоинством УКО является возможность реализации на его основе множества КО, количество которых достигает 2^m, где m есть количество разрядов осциллятора, и каждый из них определяется подаваемым запросом. В статье рассматриваются три альтернативных структуры предлагаемых ФНФ, а именно УКОФНФ$_1$, УКОФНФ$_2$ и УКОФНФ$_3$. Показываются их основные достоинства и недостатки, в том числе, в случае двух вариантов реализации, а именно на программированной логике (FPGA) и произвольной логике (ASIC). В качестве базового варианта для реализации на FPGA рассматривается УКОФНФ$_2$ менее подверженный межкристальной и, что более важно, внутрикристальной зависимости, вызванной технологическими особенностями производственного процесса. Практические исследования проводились путем реализации на современных FPGA УКОФНФ$_2$, оценки ее работоспособности и основных ее характеристик. Экспериментально подтверждена работоспособность нового класса ФНФ при их реализации на программируемой логике, а также высокие показатели их основных статистических характеристик.
Ключевые слова: физически неклонируемые функции, кольцевой осциллятор, управление частотой импульсов, счет импульсов.
Для цитирования: ИВАНЮК, Александр А.; ЯРМОЛИК, Вячеслав Н. ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫЕ ФУНКЦИИ НА БАЗЕ УПРАВЛЯЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА. Безопасность информационных технологий, [S.l.], т. 30, № 3, с. 90–103, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1532. DOI: http://dx.doi.org/10.26583/bit.2023.3.06.

Alexander A. Ivaniuk[1], Vyacheslav N. Yarmolik[2]
Belarusian State University of Informatics and Radioelectronics,
P. Brovki str., 6, Minsk, 220013, Belarus
[1]e-mail: ivaniuk@bsuir.by, https://orcid.org/0000-0002-6541-7742
[2]e-mail: yarmolik10ru@yahoo.com, https://orcid.org/0000-0003-3995-1463

Physically unclonable functions based on a controlled ring oscillator

DOI: http://dx.doi.org/10.26583/bit.2023.3.06

Abstract. The problem of constructing a new class of physically unclonable functions (PUF) based on a controlled ring oscillator (CRO) has beeb solved. The relevance of the creation of CROPUF is associated with the active development of physical cryptography used for the purposes of identifying electronic products and generating cryptographic keys. It is shown that classical physically unclonable functions based on ring oscillators (ROPUF) are characterized by large hardware redundancy due to the need to implement a large number of ROs, since each bit of the response requires an independent pair of real ROs. At the same time ROPUFs are characterized by better statistical properties compared to PUFs of the arbiter type and do not require ideal symmetry and identity of implemented ROs. As an alternative to ROPUF, a new class of physically unclonable functions is proposed, namely, CROPUF, which uses controlled ring oscillators based on controlling the frequency of generated pulses without changing the functionality and structure of the oscillator. An important advantage of the CRO is a possibility of implementing on its basis a set of ROs, the number of which reaches 2^m, where m is the number of stages of the oscillator, and each of them is determined by the submitted request. The three alternative structures for the proposed PUF, namely CROPUF1, CROPUF2 and CROPUF3 are considered. Their main advantages and disadvantages are shown, including in the case of two implementation options, namely on programmed logic (FPGA) and arbitrary logic (ASIC). As a basic option for implementation on FPGA, CROPUF2 is considered less prone to inter-chip and, more importantly, intra-chip dependence caused by the technological features of the production process. Practical studies were carried out by implementing CROPUF2 on modern FPGAs, evaluating its performance and its main characteristics. The operability of a new class of PUFs when implemented on programmable logic, as well as high rates of their main statistical characteristics, has been experimentally confirmed.

Keywords: physical unclonable functions, ring oscillator, impulse frequency control, impulse counting.
For citation: IVANIUK, Alexander A.; YARMOLIK, Vyacheslav N. Physically unclonable functions based on a controlled ring oscillator. IT Security (Russia), [S.l.], v. 30, no. 3, p. 90–103, 2023. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1532. DOI: http://dx.doi.org/10.26583/bit.2023.3.06.

Введение

Для целей идентификации и аутентификации цифровых устройств широко используются физически неклонируемые функции (ФНФ) (Physical Unclonable Functions – *PUF*), которые являются эффективным средством защиты авторского права на электронные изделия [1–2], а также активно применяются для генерирования криптографических ключей и реализации различных криптографических приложений [3–4].

Определяющим свойством физически неклонируемых функции является их неклонируемость (Unclonability), то есть невозможность воспроизведения двух ФНФ, поведение которых будет идентичным. Свойство неклонируемости таких физических систем объясняется тем, что они состоят из множества компонент характеристики которых принимают случайные значения. ФНФ описываются парой параметров, состоящей из множества входных сигналов, называемых запросом (Challenge – *C*), и соответствующих им выходных сигналов – ответов (Response – *R*). ФНФ рассматривается как функция $R = F(C)$, которая преобразует запросы *C* в ответы *R* [1, 2, 5, 6].

Существует большое множество разнообразных реализаций ФНФ на основе задержек распространения электрического сигнала, среди которых выделяются, так называемые, ФНФ типа арбитр (АФНФ – *APUF*) [5–8]. В классических АФНФ на основании запроса *C* задается конфигурация, как правило, двух функционально и топологически симметричных путей, по которым распространяются идентичные копии тестового сигнала. Ответом *R* АФНФ является результат сравнения задержек распространения сигнала по двум путям [5–8].

Определяющим недостатком АФНФ является невысокая их уникальность и стабильность в силу того, что АФНФ имеет в своей топологии систематическую асимметрию, в особенности при их реализации на программируемой логике типа FPGA [6–10]. При автоматизированном проектировании и изготовлении АФНФ достаточно

сложно управлять и контролировать симметрией всех топологических элементов, таких как длины проводников соединений, идентичность полупроводниковых элементов и их геометрических размеров, равенство задержек и др.

Значительно большей стабильностью характеризуются ФНФ на базе кольцевых осцилляторов (КОФНФ) (Ring Oscillator PUF – *ROPUF*) [4, 5, 11, 12]. Данный тип ФНФ основан на применении кольцевых осцилляторов (КО) (Ring Oscillator – *RO*), представляющих собой последовательно включенные инверторы, охваченные отрицательной обратной связью (см. рис. 1).

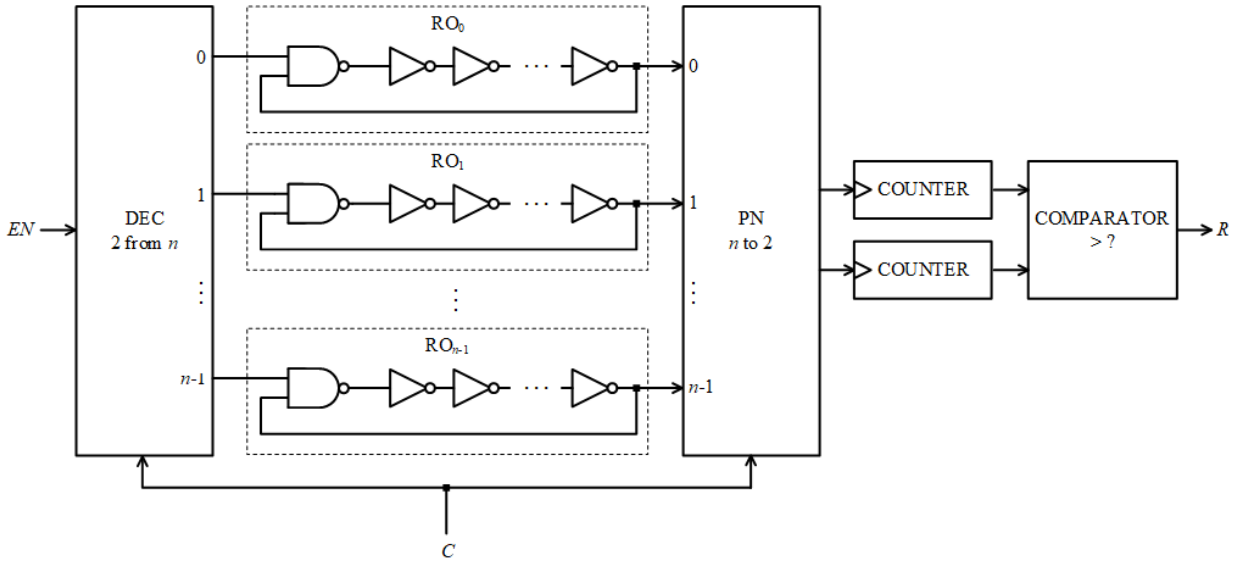


Рис. 1. Физически неклонируемая функция на базе кольцевых осцилляторов
Fig. 1. Physically unclonable function based on ring oscillators

При поступлении на первый вход элемента 2И-НЕ (см. рис. 1) единичного управляющего сигнала, и при условии, что количество инверсий в схеме RO_i, $i \in \{0, 1, \ldots, n-1\}$ нечетно, на его выходе будет формироваться импульсный сигнал. Частота формируемой импульсной последовательности определяется задержками на элементах схемы RO_i. В силу вариаций задержек сигнала на элементах осциллятора два идентичных по топологии и функциональности RO_i и RO_j, $i \neq j$ имеют отличающиеся частоты выходных импульсных сигналов [5]. Различие частот сигналов RO_i и RO_j является основой для формирования однобитного ответа *R*. Один бит ответа формируется путем сравнения частот двух кольцевых осцилляторов, которые выбираются с использованием дешифратора DEC (Decoder) с разрешением и двумя активными выходами и схемы перестановочной сети PN (Permutation Network) с *n* входами и двумя выходами. Дешифратор DEC, на основании поступившего запроса *C* и активного значения сигнала *EN*, вырабатывает на своих выходах один из C_2^n двоичных *n*-битных векторов, на двух позициях *i* и *j* ($i \neq j$) которого присутствует значение 1, на остальных – 0. При неактивном значении сигнала *EN* схема DEC вырабатывает нулевой вектор. Схема PN, на основании запроса *C*, осуществляет коммутацию уникальной пары из *n* входов с двумя своими выходами, выбирая тем самым уникальную пару RO_i и RO_j из C_2^n возможных. Выходы PN подключены ко входам двух суммирующих двоичных счетчиков (COUNTER), которые суммируют поступающие на их входы импульсы. Как отмечалось ранее, частоты импульсов поступающих от RO_i и RO_j будут отличаться. Это приводит к тому, что за фиксированный

промежуток времени (время удержания разрешающего сигнала *EN* в активном значении) содержимое счетчиков, как результат поступления импульсных последовательностей, будет различным. Причем, чем больше временной интервал, на котором проводится измерение, тем больше различие состояний двух счетчиков, что, по сути, гарантирует существенно большую стабильность функционирования ФНФ, использующих RO, по сравнению с АФНФ. Состояния двух счетчиков сравниваются на схеме сравнения (COMPARATOR), на выходе которого формируется однобитный ответ *R*. Временной интервал, в течение которого осуществляется измерение, задается путем одновременной подачи на входы двухвходовых элементов 2И-НЕ выбранных RO_i и RO_j единичного сигнала от схемы DEC.

Определяющим недостатком классической схемы КОФНФ является аппаратурная сложность их реализации, в частности сложность схем DEC и PN, требующая большого *n* числа RO для выбора их независимых пар, каждая из которых формирует только один бит ответа. Каждый RO является источником только одной уникальной частоты импульсов, которая является результатом случайных величин задержки на элементах RO.

С целью расширения функциональных возможностей ФНФ на базе КО были предложены конфигурируемые структуры КО (Configurable RO) путем замены логики каждой ступени (т.е. одного инвертора) на конфигурируемый базовый элемент, который имеет два или более вариантов значений задержки [13–16]. Однако конфигурируемые КО, как правило, ориентированы на уникальную структуру определенного типа FPGA, которая недостаточно эффективна для применения в специализированных интегральных схемах (ASIC). Более того, конфигурирование КО устанавливают зависимость задержек элементов КО от его структуры, что упрощает реализацию различного рода атак на такие ФНФ.

В настоящей статье решается задача построения нового класса КОФНФ с изменяемой частотой генерирования импульсной последовательности сигналов. Подобные ФНФ основаны на использовании КО с управляемой (изменяемой) задержкой распространения сигнала через элементы. Базовый элемент таких КО обеспечивает управляемость задержкой за счет выбора количества входов, влияющих на изменение выходного сигнала, и значений на их неактивных входах [12].

1. КОФНФ с изменяемой задержкой распространения сигнала

Все известные решения при создании ФНФ, в том числе и КОФНФ, основаны на парадигме, которая заключается в том, что задержка по конкретному пути (элементу) принимает случайное, однако неизменное и неуправляемое значение. В тоже время изменение задержки может являться результатом влияния внешних факторов таких, как температура, давление, электромагнитное излучение и др., а также результатом деградации физических и химических свойств компонент элементов, что относится к негативным и нежелательным эффектам для ФНФ.

Первые результаты построения КО с изменяемой частотой импульсной последовательности сигнала, как правило, приводили к созданию их конфигурируемых структур [13–16]. При этом достигались заметные преимущества по сравнению с классическими КОФНФ. Построение конфигурируемых КО приводило к снижению аппаратных затрат на реализацию ФНФ, так как конфигурируемый КО выполняет функции множества классических КО. Каждая его конфигурация представляет собой уникальный КО, который отличается своим схемотехническим решением и структурой от другого КО. Видоизменение схемы ФНФ является нарушением основополагающей концепции об идентичности функциональности ФНФ и их реализации, что увеличивает их уязвимость к различного рода атакам, в том числе, и с использованием машинного обучения.

В качестве альтернативного подхода для построения ФНФ в [12] обосновывается использование нового класса ФНФ с управляемыми задержками и приводятся различные варианты базовых элементов для их построения. Простейший случай базового элемента, приведенного в [12], представляет собой двухвходовой элемент XOR, один из входов которого будет представлять собой управляющий вход. При подаче на второй вход этого элемента единичного значения, выходное значение XOR изменяется на противоположное. Двоичные величины $c_i = 0$ либо $c_i = 1$, где $i \in \{0, 1, 2, \ldots, m-1\}$ на управляющем входе определяют значения задержки выходного значения i-го двухвходового элемента XOR. Последовательно подключенные двухвходовые сумматоры по модулю два представляют собой управляемый кольцевой осциллятор (УКО) (Controlled Ring Oscillator – *CRO*). В упрощенном виде данная схема приведена на рис. 2 [12].

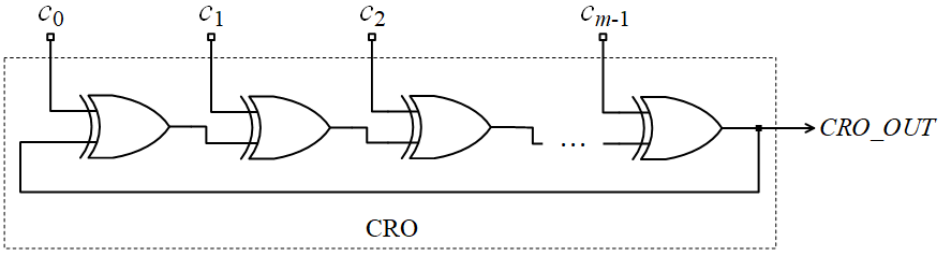


Рис. 2. Управляемый кольцевой осциллятор
Fig. 2. Controlled ring oscillator

Уникальность двухвходового элемента XOR позволяет напрямую управлять задержкой прохождения через него входного импульса путем задания произвольных входных значений 0, либо 1 по его управляющему входу. Предположив, что i-й XOR имеет задержку d_{i0} при $c_i = 0$, и задержку d_{i1} при $c_i = 1$, суммарная задержка D прохождения сигнала через m последовательно подключенных элементов УКО определяется согласно соотношению [12]:

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

Как видно из соотношения (1) временная задержка D определяется запросом $C = c_0\, c_1 \ldots c_{m-1}$ и для различных его значений принимает различные величины, представляющие суммы случайных слагаемых d_{i0} и d_{i1}. Таким образом, источником непредсказуемости и уникальности УКО являются значения задержки D, которые определяют частоты $f = 1/(2D)$ периодических сигналов, генерируемых управляемым кольцевым осциллятором на выходе *CRO_OUT*, при условии обеспечения у них отрицательной обратной связи. Необходимым и достаточным условием наличия такой связи для случая УКО, приведенного на рис. 2, является нечетное количество единичных значений c_i запроса $C = c_0\, c_1 \ldots c_{m-1}$. Таким образом, УКО, приведенный на рис. 2, позволяет сгенерировать 2^{m-1} уникальных кольцевых осцилляторов.

Управляемый КО, рассмотренный выше и приведенный на рис. 2, является наиболее простым решением управления задержками на кольцевом осцилляторе. Более сложные процессы и, соответственно, зависимости задержек через элемент возникают в случае переключения сигналов одновременно по нескольким входам (Multi Input Switching – *MIS*) базового элемента и его модификаций, представленных в [12]. Модификации исходного базового элемента позволяют управлять с помощью запроса C количеством переключающихся входных значений, которые изменяют выходное значение базового

элемента. Отметим, что не только количество входов определяется запросом *C*, но и их конкретный набор, в результате чего и происходит задание определенной задержки через каждый базовый элемент и соответственно управление величиной суммарной задержки *D* [12]. В сравнении с конфигурируемыми КО, управляемый КО позволяет управлять величиной задержки *D* не изменяя функциональность и структуру КО в зависимости от подаваемого запроса *C*.

2. Альтернативные схемы КОФНФ на базе УКО

Рассматривая классическую схему КОФНФ как основу для построения подобных функций, и осцилляторы с управляемой задержкой (УКО) как составные ее элементы, возможны различные варианты ее реализации. Первой и достаточно очевидной схемой, повторяющей схему КОФНФ, приведенную на рис. 1, является УКОФНФ$_1$, представленная на рис. 3.

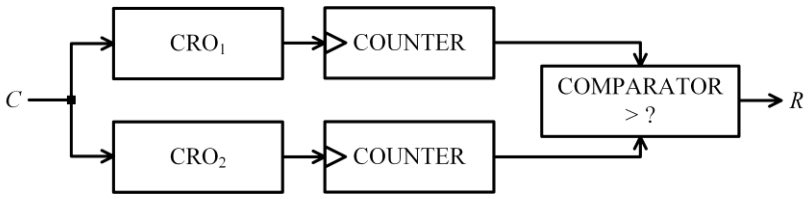


Рис. 3. Физически неклонируемая функция УКОФНФ$_1$
Fig. 3. Physically unclonable CROPUF$_1$ function

В отличие от стандартной реализации КОФНФ в схеме УКОФНФ$_1$ используются только два кольцевых осциллятора УКО$_1$ (CRO$_1$) и УКО$_2$ (CRO$_2$) с управляемой задержкой распространения сигнала. Соответственно, по конкретному запросу *C*, каждый из них выполняет функцию одного из множества осцилляторов КОФНФ (см. рис. 1). Подчеркнем, что для каждого запроса *C* УКО представляет собой уникальный КО, отличающийся от других частотой генерируемой импульсной последовательности. В остальном функционирование УКОФНФ$_1$ идентично поведению КОФНФ, описанной ранее. Как видно из приведенной структуры УКОФНФ$_1$ она характеризуется существенно меньшими аппаратными затратами по сравнению с классической реализацией КОФНФ.

Аналогично, как и для классической схемы КОФНФ, приведенной на рис. 1, для схемы УКОФНФ$_1$ также присущ недостаток, связанный с большой зависимостью частотных свойств отдельных реализаций КО в КОФНФ и УКО в УКОФНФ$_1$. В случае КОФНФ этот недостаток нивелируется большим количеством КО, для которых отличие частотных свойств является необходимым условием. При реализации УКОФНФ$_1$ физически реализуются только два УКО, которые реализуют множества КО, задаваемых запросами. Отличие частотных свойств УКО$_1$ и УКО$_2$ может приводить к ухудшению свойств УКОФНФ$_1$, а в предельном случае и к неработоспособным их версиям. Такая ситуация возможна при значительном отличии частотных свойств УКО$_1$ и УКО$_2$, когда значения частот их кольцевых осцилляторов относятся к непересекающимся диапазонам. Данная проблема присуща и для АФНФ и достаточно глубоко рассматривалась в [7, 10]. В простейшем случае, для устранения этого недостатка, необходимо решение задачи балансировки с использованием линий задержки [7, 10].

В качестве альтернативы УКОФНФ$_1$, основанной на использовании двух УКО, можно предложить структуру УКОФНФ$_2$, основанную на применении только одного УКО (CRO), рис. 4. В этом случае КО, формируемые на базе одного УКО, будут генерировать импульсные последовательности с частотами, принадлежащими одному диапазону,

определяемому структурой и реализацией УКО. Соответственно, исключается необходимость решения нетривиальной задачи балансировки [7, 10]. Кроме того, достигается сокращение аппаратурных затрат, так как в случае УКОФНФ$_2$, применяется один УКО и реверсивный счетчик (R_COUNTER).

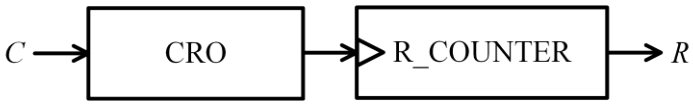


Рис. 4. Физически неклонируемая функция УКОФНФ$_2$
Fig. 4. Physically unclonable CROPUF$_2$ function

В данном случае, УКО последовательно во времени реализует два различных КО, задаваемых двумя отличными запросами *C*, подаваемыми на УКОФНФ$_2$ последовательно во времени. Для первого запроса (первый КО) реверсивный счетчик работает в режиме суммирования, а для второго запроса (второй КО) в режиме вычитания. Знак + или – содержимого указанного счетчика и определяет значение ответа *R*. По сравнению с УКОФНФ$_1$ в УКОФНФ$_2$ увеличивается в два раза время получения ответа, однако заметно увеличивается случайность, а именно равновероятность значений 0 или 1, получаемых ответов *R*. Это объясняется исключением аномальных ситуаций, когда два УКО функции УКОФНФ$_1$ формируют импульсные последовательности с частотами, принадлежащими различным, непересекающимися диапазонами частот, либо только частично пересекающимися.

Рассмотренный УКОФНФ$_2$ во многом повторяет логику работы классической схемы КОФНФ, приведенной в предыдущем разделе. Действительно, в обоих случаях на основе запросов выбираются два кольцевых осциллятора, и сравниваются частоты формируемых ими высокочастотных сигналов. При этом условно идентифицируется первый КО$_1$, частота генерируемых импульсов которого сравнивается с частотой импульсной последовательности второго КО$_2$. По результату сравнения и определяется значение ответа *R*.

Также, как и для классической схемы КОФНФ, для УКОФНФ$_2$ присущ недостаток связанный с ограничениями на количество пар КО и на их выбор. Поясним это на примере зависимости результатов при получении ответов для трех осцилляторов КО$_1$, КО$_2$ и КО$_3$, для которых рассмотрим две пары осцилляторов из трех возможных, например (КО$_1$, КО$_2$) и (КО$_2$, КО$_3$). Предположив, что в обоих случаях $R = 1$, можно заключить, что частота сигналов КО$_1$ больше частоты формируемой КО$_2$, также как и то, что КО$_2$ генерирует сигналы с большей частотой по сравнению с КО$_3$. Отсюда следует, что пара (КО$_1$, КО$_3$) так же сформирует ответ $R = 1$, так как частота импульсных сигналов у КО$_1$ больше чем у КО$_3$ и выбор данной пары не позволяет извлечь дополнительной информации о поведении УКОФНФ$_2$.

Для получения оценок количества независимых пар КО формируемых *m*-разрядным УКОФНФ$_2$ можно использовать результаты хорошо изученных и применяемых на практике алгоритмов сортировки [17, 18]. Также, как и в УКОФНФ$_2$ и КОФНФ, все алгоритмы сортировки массивов основаны на сравнении двух элементов, при этом данная операция определяет сложность алгоритмов сортировки. Выбор пар элементов при процедуре сортировки влияет на его временную сложность, которая оценивается минимальным и максимальным значениями [18]. Эти величины определяют минимальное (Q_{min}) и максимальное (Q_{max}) значение количества сравниваемых пар элементов, необходимых для сортировки их элементов. В случае КОФНФ и УКОФНФ$_2$ указанные

оценки позволяют определить количество независимых пар КО, которые формируют независимые ответы *R*. Используя результаты, полученные для самых быстрых известных универсальных алгоритмов сортировки [17, 18], оценки $Q_{\min}$ и $Q_{\max}$ для количества пар независимых КО формируемых УКОФНФ$_2$, на базе УКО (рис. 2), примут вид:

$$Q_{\min} = 2^{m-1}\log_2 2^{m-1} = (m-1)2^{m-1}; \quad Q_{\max} = (2^{m-1})(2^{m-1}) = 2^{2m-2}. \qquad (2)$$

Как видно из соотношений (2) количества независимых пар КО даже для небольших *m* принимает большое значение, что позволяет заметно упростить выборку необходимого количества пар.

Стабильность и качество функционирования КОФНФ и УКОФНФ во многом определяется схемой формирования окна измерения, которое задает временной интервал подсчета высокочастотных импульсов, формируемых КО. Как показано в [19] весьма важным является реализация схемы, определяющей окно измерения и КОФНФ в одной и той же области кристалла и, что более важно, в одной и той же области источника питания. При этом сама схема окна захвата строилась на КО, что предопределяло синхронное влияние внешних факторов на частотные свойства как самой КОФНФ, так и схемы, определяющей временное окно измерений количества импульсов. Таким образом, формирование окна измерения на кристалле смогло решить проблему низкой повторяемости ответов при колебаниях напряжения питания вызванных негативными внешними факторами [19].

Руководствуясь результатами работ [19–21] по достижению высокой повторяемости при реализации физически неклонируемых функций PL-PUF, можно предложить третью модификацию физически неклонируемой функции, а именно управляемый кольцевой осциллятор УКОФНФ$_3$. Отличие новой модификации от предыдущей УКОФНФ$_2$ заключается в использовании вместо реверсивного счетчика стандартного многоразрядного двоичного счетчика. Очевидно, что состояние счетчика при повторении эксперимента с одним и тем же значением запроса и при достижении высокой степени повторяемости должно быть стабильным. Это, в свою очередь, позволяет использовать в качестве ответа на один запрос более одного бита результирующего состояния счетчика. Принимая во внимание разную степень стабильности значений разрядов состояний счетчика, в качестве ответов могут использоваться младшие разряды, стабильность которых принимает приемлемые значения.

В предельном случае возможно даже применение одноразрядного двоичного счетчика, представляющего собой Т-триггер. Используемый триггер определяет четность либо нечетность количества импульсов, формируемых на выходе УКО за выбранное временное окно измерений. Как показано в работах [19–21], и в подобном случае, возможно достижение высокой степени повторяемости. Очевидно, что данный предельный случай УКОФНФ$_3$, также, как и сама идея получения на его основе многоразрядного ответа, может быть реализована на ASIC, в то время как УКОФНФ$_2$ – на FPGA. В случае УКОФНФ$_2$ нет необходимости соблюдения строгой идентичности и симметричности реализуемых устройств.

3. Экспериментальные исследования УКОФНФ

Техническая часть экспериментального исследования заключалась в реализации схемы конфигурируемого кольцевого осциллятора УКОФНФ$_2$ (см. рис. 4) на ПЛИС типа FPGA Xilinx Zynq-7000 (xc7z010clg400-1), входящей в состав платы быстрого прототипирования Digilent ZYBO Z7-10. Управление осциллятором, первичный сбор и

передача данных осуществлялись программным способом при помощи встроенного в ПЛИС процессорного ядра ARM Cortex A9. Последующий анализ экспериментальных данных проводился на языке Python в среде JupyterLab.

На рис. 5 приведена структурная схема УКО, описанная ранее, (см. рис. 2), и являющаяся базовой для реализованной УКОФНФ$_2$. Схема включает в себя m=8 сумматоров по модулю 2 (sXOR2$_0$ – sXOR2$_7$), схему коррекции, состоящую из синхронного триггера FDCE, инвертора RTL_INV и дополнительного элемента sXOR2$_8$. Логический элемент RTL_AND, замыкающий цепь обратной связи осциллятора, служит для его управления в старт-стопном режиме.

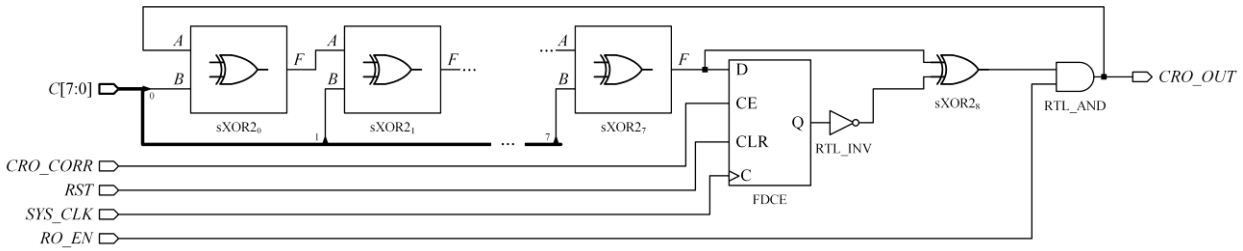


Рис. 5. Структурная схема конфигурируемого кольцевого осциллятора
Fig. 5. Structural diagram of a configurable ring oscillator

Представленная схема на рис. 5, в отличии от схемы на рис. 2, посредством схемы коррекции запроса C позволяет задавать в общем случае произвольную конфигурацию УКО из 2^m возможных. При этом выполнение процедуры коррекции необходимо для каждого подаваемого запроса перед разрешением функционирования осциллятора.

Для увеличения описанного ранее эффекта управления задержкой прохождения импульсов в схеме УКО элементы XOR (sXOR2$_0$ – sXOR2$_7$) были реализованы при помощи трех технологических LUT-блоков, в то время как корректирующий элемент sXOR2$_8$ – на одном LUT блоке.

Входная шина C [7:0] служит для конфигурации одного из 256 возможных кольцевых осцилляторов. Для обеспечения нечетного числа инверсий в кольце осциллятора предусмотрена схема коррекции, которая конфигурирует дополнительный элемент sXOR2$_8$ в качестве повторителя либо инвертора. После задания конфигурации и проведения процедуры коррекции активное значения на входе RO_EN=’1’ запускает процесс осцилляции и на выходе *CRO_OUT* наблюдается периодический сигнал с уникальной частотой *f*, для подсчета которой использовался синхронный 32-разрядный счетчик с прямым и обратным счетом.

В ходе проведенных экспериментов последовательно конфигурировались все возможные пары различных осцилляторов RO_i и RO_j $(i \neq j)$ при помощи генератора псевдослучайной последовательности, построенного на основе LFSR-структуры с характеристическим полиномом $\varphi(x) = x^8 + x^6 + x^5 + x^4 + 1$.

Для выбранной m-й пары осцилляторов из M возможных осуществлялось сравнение их частот с выработкой бинарного ответа $r_m \in \{0,1\}$ в заданном временном окне измерения $TMW = k \cdot P_{SYS\_CLK}$, где k есть целочисленный коэффициент масштабирования, P_{SYS_CLK} – период системного сигнала синхронизации. Сравнение частот осуществлялось следующим образом: для первого сконфигурированного генератора счетчик, подключенный к выходу RO_OUT, осуществлял прямой счет числа сгенерированных импульсов в заданном окне

измерения. Для второго генератора счетчик переводился в режим обратного счета. После окончания измерения положительное значение счетчика свидетельствует о большей частоте первого генератора $f(RO_i) > f(RO_j)$, отрицательное же значение счетчика – о большей частоте второго генератора $f(RO_i) < f(RO_j)$.

В случае, если $f(RO_i) > f(RO_j)$, то вырабатывался нулевой ответ $r_m = 0$, в противном случае – единичный ответ $r_m = 1$. Выработка ответа для каждой пары осцилляторов повторялась $E = 100$ с подсчетом суммы $S = \sum_{e=1}^{E} r_m$. Если $S = 0$, то фиксировался стабильный нулевой ответ, в случае если $S = E$ – стабильный единичный ответ, а при условии $0 < S < E$ – ответ фиксировался как метастабильный.

Для заданного k и всех возможных M пар генераторов осуществлялся подсчет числа нулевых R_0, единичных R_1 и метастабильных R_x ответов.

На рис. 6 приведены графики процентного отношения нулевых $N_0 = 100 \cdot R_0 / M$, единичных $N_1 = 100 \cdot R_1 / M$ и метастабильных ответов $N_x = 100 \cdot R_x / M$ ко всем возможным ответам *M* в зависимости от коэффициента масштабирования *k* временного окна измерения *TMW*.

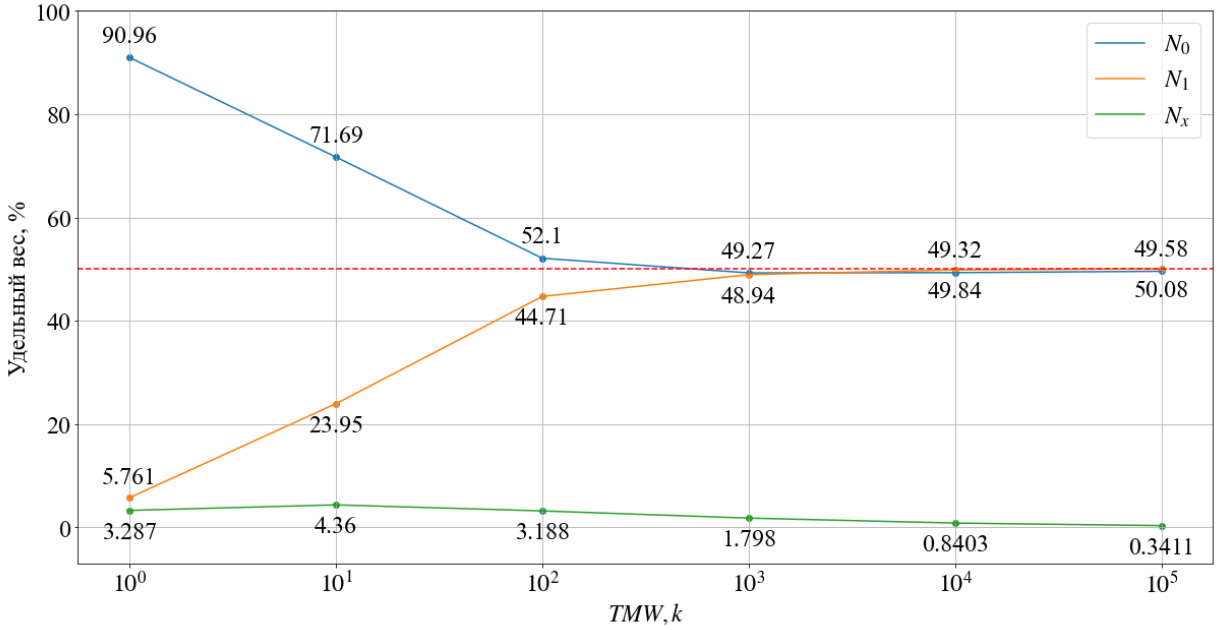


Рис. 6. Распределение ответов в зависимости от коэффициента k
Fig. 6. Distribution of answers depending on the coefficient k

Как видно из представленных графиков начиная со значения $k = 10^3$ и далее удельные веса нулевых N_0 и единичных N_1 ответов практически совпадают и начинают незначительно изменяться с увеличением *k*, и достигают значений 49,58% и 50,08% соответственно при $k = 10^5$. При малых значениях $k < 10^2$ частоты большинства конфигурируемых генераторов являются неразличимыми.

В свою очередь удельный вес метастабильных ответов достигает максимума в 4,36% при $k = 10^1$, а с дальнейшим ростом окна измерения начинается уменьшаться, и для $k = 10^5$ уже составляет 0,34% для всех возможных сравниваемых пар генераторов.

Таким образом, можно констатировать, что размер окна измерения частот УКО с коэффициентом масштабирования $k=10^3$ является достаточным для реализации схемы ФНФ с хорошими показателем стабильности. Не менее значимой характеристикой для схем ФНФ является единообразие (Uniformity), которая показывает степень равенства мощностей множеств нулевых и единичных ответов.

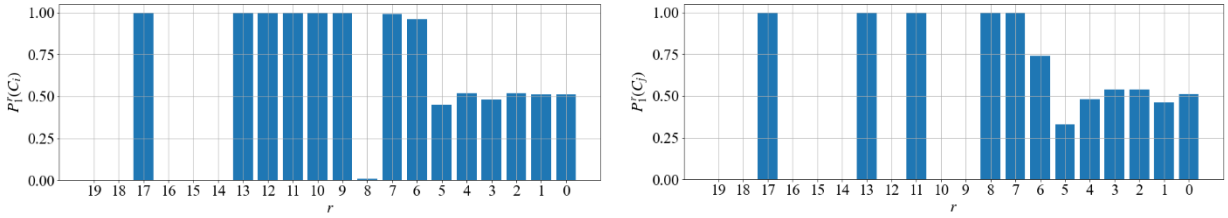
В табл. 1 приведены значения характеристик стабильности (*St*) и единообразия (*Un*) для различных значений *k*.

Таблица 1. Основные характеристики УКОФНФ$_2$

Характеристики	Коэффициент масштабирования окна измерения, *k*					
	10^0	10^1	10^2	10^3	10^4	10^5
St	0,9671	0,9564	0,9681	0,9820	0,9915	0,9965
Un	0,1152	0,4790	0,8942	0,9787	0,9968	0,9983

Состоятельность идеи реализации схемы УКОФНФ$_3$ продемонстрируем следующим результатом, полученным на основе реализованной схемы УКО (см. рис. 5) и 20-разрядным двоичным счетчиком прямого счета.

На E=100 экспериментах при выбранном фиксированном окне измерения k проводился анализ значений вероятности $P_1^r(C)$ появления единичного символа на каждом r-м разряде ($r\in[0,19]$) счетчика при подаче одного и того же значения запроса C. На рис. 7 представлены значения $P_1^r(C)$ для k=10^5 и двух запросов $C_i \neq C_j$.



а) *б*)

Рис. 7. Значения вероятности $P_1^r(C)$ для запроса C_i (а) и C_j (б)

Fig. 7. The value of the probability $P_1^r(C)$ for challenge C_i (a) and for C_j (b)

Как видно из приведенных графиков для запроса C_i наблюдается 11 старших разрядов счетчика $r\in[9,19]$, значения для которых стабильны на E повторениях. Для запроса C_j наблюдается 13 подобных разрядов ($r\in[7,19]$). Выбирая для двух запросов 11 старших разрядов (два из которых незначимы для r=18 и r=19) можно сформировать два стабильных многоразрядных ответа R_i = 00100011111 и R_j = 00100010100, которые несут больше информации в сравнении со схемой, определяющей только однобитный результат неравенства.

Приведенные результаты экспериментальных исследований свидетельствуют о состоятельности предложенных ФНФ на основе схем УКО.

Заключение

В настоящей статье приведены исследования нового класса КОФНФ основанного на применении кольцевых осцилляторов с управляемой (изменяемой) частотой генерирования импульсной последовательности сигналов. Приводятся альтернативные структуры

КОФНФ, а именно: УКОФНФ$_1$, УКОФНФ$_2$ и УКОФНФ$_3$. Показываются их основные достоинства и недостатки, в том числе, в случае двух вариантов реализации, а именно на программированной логике (FPGA) и произвольной логике (ASIC). В качестве базового варианта для реализации на FPGA рассматривается УКОФНФ$_2$ менее подверженный межкристальной и, что более важно, внутрикристальной зависимости, вызванной технологическими особенностями производственного процесса. Практические исследования проводились путем реализации на современных FPGA УКОФНФ$_2$, оценки ее работоспособности и основных ее характеристик.

Экспериментально подтверждена работоспособность нового класса ФНФ при их реализации на программируемой логике, а также высокие показатели их основных статистических характеристик. Интересным представляется дальнейшее исследование УКОФНФ, реализованных на других типах FPGA, и как ASIC с различными технологическими нормами и особенностями.

СПИСОК ЛИТЕРАТУРЫ:

1. Rührmair U., Busch H., Katzenbeisser S. Strong PUFs: models, constructions, and security proofs. Towards Hardware-Intrinsic Security. Editors: A.-R. Sadeghi, D. Naccache. Berlin, Heidelberg: Springer Berlin Heidelberg. 2010, p. 79–96. DOI: http://dx.doi.org/10.1007/978-3-642-14452-3.
2. Дураковский Анатолий П.; Кессаринский Леонид Н.; Ширин Алексей О. Маркировка и проверка подлинности изделий микроэлектроники на основе неклонируемости радиационного поведения. Безопасность информационных технологий, [S.l.], т. 27, № 3, с. 18–25, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.3.02. – EDN OJDTLM.
3. Lim D., Lee J.W., Gassend B., Suh T.G., Dijk M.V., Devadas S. Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no. 10, p. 1200-1205, Oct. 2005 DOI: http://dx.doi.org/10.1109/TVLSI.2005.859470.
4. Lee J.W., Lim D., Gassend B., Suh T.G., Dijk M.V., Devadas S. A technique to build a secret key in integrated circuits for identification and authentication applications. Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), Honolulu, HI, USA, 2004, p. 176–179. DOI: http://dx.doi.org/10.1109/VLSIC.2004.1346548.
5. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонируемые функции. Информатика. 2011, т. 30, № 2, с. 92–103. – EDN RBYGUD.
6. Böhm C., Hofer M. Physical Unclonable Functions in Theory and Practice. N. Y.: Springer Science + Business Media, 2013. – 278 p. DOI: http://dx.doi.org/.1007/978-1-4614-5040-5_10.
7. Ярмолик Вячеслав Н.; Иванюк Александр А. Сбалансированные физически неклонируемые функции типа арбитр. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 92–107, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.07. – EDN HCUPGE.
8. Ярмолик В.Н., Иванюк А.А. Двухмерные физически неклонируемые функции типа арбитр. Информатика. 2023, т. 20, № 1, с. 7–26. DOI: https://doi.org/10.37661/1816-0301-2023-20-1-7-26.
9. Morozov S., Maiti A., Schaumont P. (March 2010) An Analysis of Delay Based PUF Implementations on FPGA. In: Sirisuk, P., Morgan, F., El-Ghazawi, T., Amano, H. (eds) Reconfigurable Computing: Architectures, Tools and Applications. ARC 2010. Lecture Notes in Computer Science, vol 5992. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-12133-3_37.
10. Ярмолик В.Н., Иванюк А.А. Физически неклонируемые функции типа арбитр с заведомо асимметричными парами путей. Доклады БГУИР. 2022, т. 20, № 4, с. 71–79. DOI: https://doi.org/10.35596/1729-7648-2022-20-4-71-79.
11. Qu G., Yin C.-E. Temperature-aware cooperative ring oscillator PUF. IEEE International Workshop on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 2009, p. 36–42. DOI: https://doi.org/10.1109/HST.2009.5225055.
12. Ярмолик В.Н., Иванюк А.А., Шинкевич Н.Н. Физически неклонируемые функции с управляемой задержкой распространения сигналов. Информатика. 2022, т. 19, № 1, с. 32–49. DOI: https://doi.org/10.37661/1816-0301-2022-19-1-32-49.
13. Maiti A., Schaumont P. Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators. International Conference on Field Programmable Logic and Applications, Prague, Czech Republic. 2009, p. 703–707. DOI: https://doi.org/10.1109/FPL.2009.5272361.

14. Xin X., Kaps J.-P., Gaj K. A Configurable Ring-Oscillator-Based PUF for Xilinx FPGAs. 14th Euromicro Conference on Digital System Design, Oulu, Finland. 2011, p. 651–657. DOI: https://doi.org/10.1109/DSD.2011.88.
15. Deng D., Hou S., Wang Z. Guo Y. Configurable Ring Oscillator PUF Using Hybrid Logic Gates. IEEE Access, vol. 8, p. 161427–161437, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3021205.
16. Liu W., Zhang L., Zhang Z., Gu C., Wang C., O'neill M., Lombardi F. 2019. XOR-Based Low-Cost Reconfigurable PUFs for IoT Security. ACM Trans. Embed. Comput. Syst. 18, 3, Article 25 (May 2019), 21 p. DOI: https://doi.org/10.1145/3274666.
17. Hoare C. A. R. Algorithm 64: Quicksort. Communications of the ACM. 1961, vol. 4, no. 7, p. 321. DOI: https://doi.org/10.1145/366622.366644.
18. Bentley J.L., McIlroy M.D. Engineering a sort functions. Software-Practice and Experience. 1993, vol. 23, no. 11, p. 1249–1265. DOI: https://doi.org/10.1002/spe.4380231105.
19. Ogasahara Y., HoriY., Katashita T., Iizuka T., Awano H., Ikeda M., Koike H. Implementation of pseudo-linear feedback shift register-based physical unclonable functions on silicon and sufficient Challenge – Response pair acquisition using Built-In Self-Test before shipping. Integration. 2020, vol. 71, p. 144–153. DOI: https://doi.org/10.1016/j.vlsi.2019.12.
20. Hori Y., Kang H., Katashita T., Satoh A. (Nov. 2011) Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function. International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico. 2011, p. 223–228. DOI: https://doi.org/10.1109/ReConFig.2011.72.
21. Ogasahara Y., Hori Y., Koike H., (May 2016), May. Implementation of pseudo linear feedback shift register physical unclonable function on silicon. IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada. 2016, p. 758–761. DOI: https://doi.org/10.1109/ISCAS.2016.7527351.

REFERENCES:

[1] Rührmair U., Busch H., Katzenbeisser S. Strong PUFs: models, constructions, and security proofs. Towards Hardware-Intrinsic Security. Editors: A.-R. Sadeghi, D. Naccache. Berlin, Heidelberg: Springer Berlin Heidelberg. 2010, p. 79–96. DOI: http://dx.doi.org/10.1007/978-3-642-14452-3.
[2] Durakovskiy Anatoly P.; Kessarinskiy Leonid N.; Shirin Alexey O. The use of microelectronics radiation behavior asphysical uncloned function to find counterfeit. IT Security (Russia), [S.l.], v. 27, no. 3, p. 18–25, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.3.02 (in Russian). – EDN OJDTLM.
[3] Lim D., Lee J.W., Gassend B., Suh T.G., Dijk M.V., Devadas S. Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 13, no. 10, p. 1200-1205, Oct. 2005 DOI: http://dx.doi.org/10.1109/TVLSI.2005.859470.
[4] Lee J.W., Lim D., Gassend B., Suh T.G., Dijk M.V., Devadas S. A technique to build a secret key in integrated circuits for identification and authentication applications. Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525), Honolulu, HI, USA, 2004, p. 176–179. DOI: http://dx.doi.org/10.1109/VLSIC.2004.1346548.
[5] Yarmolik V.N., Vashinko Y.G. Physical unclonable functions. Informatics. 2011, v. 30, no. 2, p. 92–103 (in Russian). – EDN RBYGUD.
[6] Böhm C., Hofer M. Physical Unclonable Functions in Theory and Practice. N. Y.: Springer Science + Business Media, 2013. – 278 p. DOI: http://dx.doi.org/.1007/978-1-4614-5040-5_10.
[7] Yarmolik Vyacheslav N.; Ivaniuk Alexander A. Balanced arbiter physical uncloneable functions. IT Security (Russia), [S.l.], v. 30, no. 1, p. 92–107, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.07 (in Russian). – EDN HCUPGE.
[8] Yarmolik V.N., Ivaniuk A.A. 2D physically unclonable functions of the arbiter type. Informatics. 2023, v. 20, no. 1, p. 7–26. URL: https://doi.org/10.37661/1816-0301-2023-20-1-7-26 (in Russian).
[9] Morozov S., Maiti A., Schaumont P. (March 2010) An Analysis of Delay Based PUF Implementations on FPGA. In: Sirisuk, P., Morgan, F., El-Ghazawi, T., Amano, H. (eds) Reconfigurable Computing: Architectures, Tools and Applications. ARC 2010. Lecture Notes in Computer Science, vol 5992. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-642-12133-3_37.
[10] Yarmolik V.N., Ivaniuk A.A. Arbiter Physical Unclonable Functions with Asymmetric Pairs of Paths. Doklady BGUIR. 2022, v. 20, no. 4, p. 71–79. DOI: https://doi.org/10.35596/1729-7648-2022-20-4-71-79 (in Russian).
[11] Qu G., Yin C.-E. Temperature-aware cooperative ring oscillator PUF. IEEE International Workshop on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 2009, p. 36–42. DOI: https://doi.org/10.1109/HST.2009.5225055.
[12] Yarmolik V.N., Ivaniuk A.A., Shynkevich N.N. Physically unclonable functions with controlled propagation delay. Informatics. 2022, v. 19, no. 1, p. 32–49. DOI: https://doi.org/10.37661/1816-0301-2021-19-1-32-49 (in Russian).

[13] Maiti A., Schaumont P. Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators. International Conference on Field Programmable Logic and Applications, Prague, Czech Republic, 2009, p. 703–707. DOI: https://doi.org/10.1109/FPL.2009.5272361.

[14] Xin X., Kaps J.-P., Gaj K. A Configurable Ring-Oscillator-Based PUF for Xilinx FPGAs. 14th Euromicro Conference on Digital System Design, Oulu, Finland. 2011, p. 651–657. DOI: https://doi.org/10.1109/DSD.2011.88.

[15] Deng D., Hou S., Wang Z. Guo Y. Configurable Ring Oscillator PUF Using Hybrid Logic Gates. IEEE Access, vol. 8, p. 161427–161437, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3021205.

[16] Liu W., Zhang L., Zhang Z., Gu C., Wang C., O'neill M., Lombardi F. 2019. XOR-Based Low-Cost Reconfigurable PUFs for IoT Security. ACM Trans. Embed. Comput. Syst. 18, 3, Article 25 (May 2019), 21 p. DOI: https://doi.org/10.1145/3274666.

[17] Hoare C. A. R. Algorithm 64: Quicksort. Communications of the ACM. 1961, vol. 4, no. 7, p. 321. DOI: https://doi.org/10.1145/366622.366644.

[18] Bentley J.L., McIlroy M.D. Engineering a sort functions. Software-Practice and Experience. 1993, vol. 23, no. 11, p. 1249–1265. DOI: https://doi.org/10.1002/spe.4380231105.

[19] Ogasahara Y., HoriY., Katashita T., Iizuka T., Awano H., Ikeda M., Koike H. Implementation of pseudo-linear feedback shift register-based physical unclonable functions on silicon and sufficient Challenge – Response pair acquisition using Built-In Self-Test before shipping. Integration. 2020, vol. 71, p. 144–153. DOI: https://doi.org/10.1016/j.vlsi.2019.12.

[20] Hori Y., Kang H., Katashita T., Satoh A. (Nov. 2011) Pseudo-LFSR PUF: A Compact, Efficient and Reliable Physical Unclonable Function. International Conference on Reconfigurable Computing and FPGAs, Cancun, Mexico. 2011, p. 223–228. DOI: https://doi.org/10.1109/ReConFig.2011.72.

[21] Ogasahara Y., Hori Y., Koike H., (May 2016), May. Implementation of pseudo linear feedback shift register physical unclonable function on silicon. IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada. 2016, p. 758–761. DOI: https://doi.org/10.1109/ISCAS.2016.7527351.

Поступила в редакцию – 02 августа 2023 г. Окончательный вариант – 27 августа 2023 г.
Received – August 02, 2023. The final version – August 27, 2023.