УДК 004.312
doi: 10.26583/bit.2024.2.08

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

КОНФИГУРИРУЕМЫЙ КОЛЬЦЕВОЙ ОСЦИЛЛЯТОР С УПРАВЛЯЕМЫМИ МЕЖСОЕДИНЕНИЯМИ

Аннотация. Рассматриваются схемотехнические решения для реализации физически неклонируемых функций (ФНФ) кольцевого осциллятора (КО) для целей идентификации цифровых устройств, генерирования криптографических ключей и последовательностей случайных чисел. Эффективность применения конфигурируемых КО (ККО) в схемах ФНФ, заключается не только в сокращении аппаратных затрат на реализацию традиционных ФНФ КО, но и в обеспечении генерирования выходных сигналов с близкими по значению уникальными частотами при реализации на ПЛИС типа FPGA. В статье предлагается модификация базовой схемы ФНФ ККО, основанной на использовании элементов XOR2, выполняющих роль элементов управляемой задержки, для которой, в отличие от базовой схемы, возможно применение полного множества запросов. Показано, что задержка зависит не только от значения запроса, но и от конфигурации межсоединений структурных элементов схемы ККО. Предлагается временная модель модифицированной ФНФ ККО, позволяющая аналитически доказать влияние межсоединений на частоту вырабатываемого сигнала, которое было экспериментально подтверждено с использованием FPGA Xilinx серии Zynq-7000. На основе этого результата предложена новая структура ФНФ ККО с управляемыми межсоединениями.
Ключевые слова: физически неклонируемые функции, кольцевой осциллятор, межсоединения.
Для цитирования: ИВАНЮК, Александр А.; ЯРМОЛИК, Вячеслав Н. КОНФИГУРИРУЕМЫЙ КОЛЬЦЕВОЙ ОСЦИЛЛЯТОР С УПРАВЛЯЕМЫМИ МЕЖСОЕДИНЕНИЯМИ. Безопасность информационных технологий, [S.l.], т. 31, № 2, с. 121–133, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1633. DOI: http://dx.doi.org/10.26583/bit.2024.2.08.

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

Configurable ring oscillator with controlled interconnections

Abstract. Circuit solutions for physically unclonable functions (PUF) of a ring oscillator (RO) implementation for the purposes of digital devices identification, cryptographic keys and random numbers generation are considered. The effectiveness using configurable ROs (CROs) in PUF circuits is based not only on reducing of the hardware overhead of traditional RO PUFs, but also on the generation of output signals with unique frequencies, close in value in a case of the FPGA implementation. The proposed modification of the basic scheme of the CRO PUF, based on the XOR2 logic gates as controlled delay elements, allows to use a full set of input challenges instead of the basic scheme. It is shown that the delay value depends not only on the challenge, but also on the interconnect configuration of the structural elements of the CRO circuit. A time model of the modified CRO PUF is proposed, which analytically proves the influence of interconnects on the frequency of the generated signal, which was experimentally

confirmed using the Xilinx Zynq-7000 FPGA. Based on this result, a new structure of PUF CRO with controlled interconnections is proposed.
Keywords: physical unclonable functions, ring oscillator, interconnections.
For citation: IVANIUK, Alexander A.; YARMOLIK, Vyacheslav N. Configurable ring oscillator with controlled interconnections. IT Security (Russia), [S.l.], v. 31, no. 2, p. 121–133, 2024. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1633. DOI: http://dx.doi.org/10.26583/bit.2024.2.08.

Введение

Физически неклонируемые функции (ФНФ) являются базовыми примитивами физической криптографии, используемые для таких задач, как неклонируемая идентификация и аутентификация цифровых устройств, построение аппаратных систем защиты от клонирования и обратного проектирования, для реализации схем генерирования случайных чисел и т.п. [1]. Среди всего многообразия типов ФНФ можно выделить ФНФ кольцевого осциллятора (КО) [2], вырабатывающего на своем выходе периодический сигнал с уникальной частотой, значение которой можно легко оценить, но практически невозможно воспроизвести. Классическая цифровая схема ФНФ КО состоит из M однотипных по структуре КО, вырабатывающих сигналы с близкими, но принципиально различными частотами, значениями которых невозможно управлять. Из всего множества пар КО соответствующим образом по значению запроса C выбираются две схемы КО, вырабатываемые частоты которых сравниваются. Результат сравнения формирует однобитный ответ R всей схемы ФНФ. Таким образом, ФНФ КО реализует функцию $R=PUF_{RO}(C)$, для которой множество пар «запрос-ответ» $\{C, R\}$ является случайным, уникальным и неклонируемым при достаточно большом M. Одним из основных недостатком классической схемы ФНФ КО является сильно возрастающая аппаратная сложность схемы выборки пары КО для анализа с увеличением значения M, а при реализации множества схем КО на программируемой логике типа FPGA, в силу исходной асимметрии конфигурируемых ресурсов, наблюдается значительное отличие анализируемых частот, что приводит к детерминированным ответам схемы ФНФ [3].

Для устранения проблем классической схемы исследователями в области ФНФ КО предлагаются различные решения, в частности замена множества схем КО одной схемой конфигурируемого КО (ККО) [4], вырабатывающего выходные сигналы близкие по частотам, но принципиально различные. Для одной схемы ККО возможно воспроизведение функционала классической ФНФ КО, когда сравнению подвергаются две частоты, выработанные одной схемой ККО с двумя различными значениями конфигурации. С учетом того, что анализ частоты практически во всех схемах ФНФ осуществляется синхронным двоичным счетчиком (проводится подсчет числа сгенерированных импульсов в фиксированном временном окне измерения), его конечное значение может быть использовано как многобитный ответ на запрос-конфигурацию ККО. В такой конфигурации возможно решение дополнительных задач – уникальной идентификации по старшим более стабильным разрядам счетчика, и генерации случайных чисел, используя младшие разряды [3].

В данной статье предлагается новая схема, основанная на уникальности не только всей схемы ККО, а и его структурных элементов путем управления их межсоединениями, что увеличивает мощность множества пар «запрос-ответ» в контексте использования схемы в качестве ФНФ.

1. ФНФ кольцевого осциллятора

Для устранения проблем классической ФНФ КО предложено много схемотехнических решений, среди которых можно выделить решения, основанные на применении так называемых конфигурируемых КО (ККО), общая структура которого представлена на рис. 1.а.

Схема ККО (CRO, Configurable Ring Oscillator) состоит из двух основных структурных блоков: логического элемента NAND, обеспечивающего старт-стопный режим работы по активному высокому уровню сигнала разрешения *EN*, и блока программируемой задержки PD, управляемого сигналами входной *n*-разрядной шины *C*, позволяющего формировать 2^n различных значений задержек сигнала $\Delta(C)$.

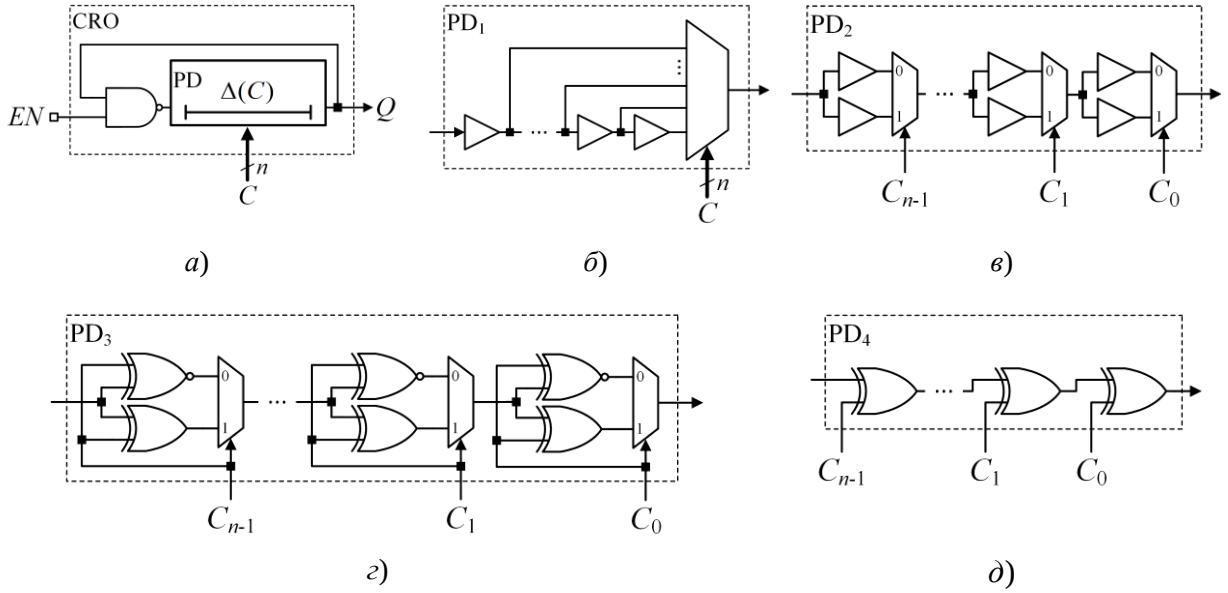


Рис. 1. Общая структура ККО (а) и альтернативные схемы программируемых элементов задержки (б, в, г, д)

При единичном сигнале *EN*=1 и фиксированном значении *C* схема конфигурируется в кольцевой осциллятор, вырабатывающий на выходе *Q* периодический сигнал с уникальной частотой $F_Q(C)$ из 2^n возможных.

Одной из простейших схем программируемой задержки (PD, Programmable Delay) является схема PD_1 (рис. 1.б), состоящая из 2^n буферов-повторителей и 2^n-входового мультиплексора, к селективным входам которого подключена шина *C* [5]. Основным недостатком данной схемы является генерирование выходного сигнала с частотой, значение которой линейно зависит от двоичного кода на шине *C*, выбирающий один из возможных заведомо неравнозначных путей. Кроме этого, схема обладает большими аппаратными затратами как на реализацию буферов, так и на схему мультиплексора и может быть применена только в классической схеме ФНФ КО, когда сравнению подвергаются близкие по значению частоты различных ККО, либо в схемах генерирования неклонируемых идентификаторов [6].

Следующая схема PD_2 (рис. 1.в) имеет линейную структуру и состоит из *n* двухвходовых мультиплексоров и 2*n* буферов [7], и, как предыдущая схема, способна вырабатывать 2^n частот, результат сравнения которых является непредсказуемым в силу схожих, но принципиально различных, конфигурируемых путей. Аналогичная архитектурная идея лежит в основе построения схемы PD_3 (рис. 1.г) [8], где вместо буферов

используются конфигурируемые инверторы, роль которых выполняют элементы XOR2 и NXOR2, которые дополнительно генерируют неуправляемые задержки для выбираемых путей. Однако подобные схемы обладают большими аппаратными затратами и меньшей степенью схожести конфигурируемых путей, что накладывает особые ограничения на применяемые значения C.

Идея использования управляемых задержек на элементах схем программируемой задержки лежит в основе более компактной, с точки зрения аппаратных ресурсов и меньшей степенью предсказуемости результата сравнения генерируемых частот, схемы PD_4 (рис. 1.д) [3]. Схема представляет собой последовательно соединенные элементы XOR2, каждый из которых выполняет роль конфигурируемого инвертора, настраиваемого соответствующим разрядом шины C. Как было показано в [3, 9] элемент XOR2, в зависимости от фиксированного значения на одном из своих входов, выполняет сам роль элемента управляемой задержки. Данная схема также имеет ограничение на используемые значения C, которые должны выбираться так, чтобы число сконфигурируемых инверторов было нулевым либо четным (с учетом использования NAND элемента), для обеспечения работы всей схемы ККО. Это уменьшает мощность множества используемых значений C до 2^{n-1}. Для возможности использования полноценного множества C была предложена схема [3], обладающая при этом дополнительными аппаратными и временными издержками на реализацию и функционирование всей схемы ККО.

В данной работе предлагается альтернативная схема ККО, основанная на идее управляемой коммутации входов элементов XOR2 в схеме программируемой задержки PD_4 и не требующая дополнительной корректирующей аппаратуры для возможности применения всего множества n-разрядных запросов C.

2. Предлагаемая схема ККО

Предлагаемая схема имеет симметричную структуру и, в простейшем случае для n=1, содержит два элемента XOR2 (рис. 2.а). Для упрощения дальнейших рассуждений будем рассматривать схему ККО без дополнительного логического элемента NAND, обеспечивающего старт-стопный режим работы.

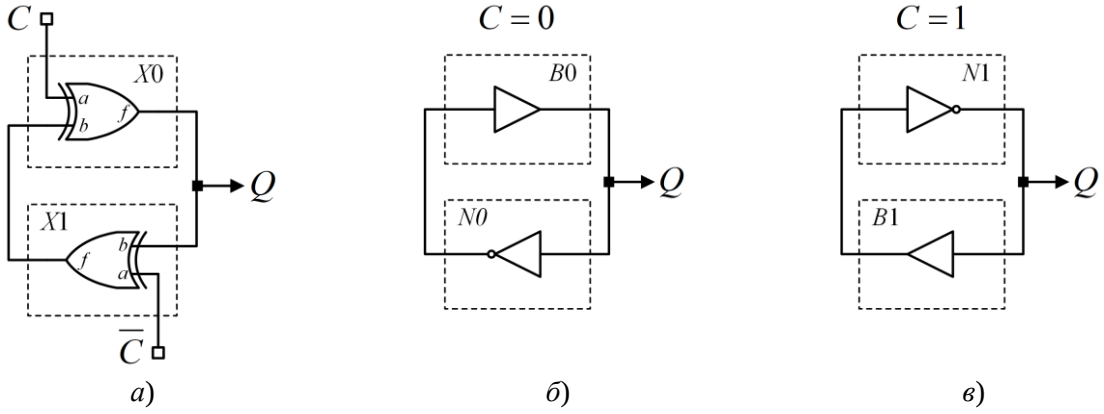


Рис. 2. Предлагаемая схема ККО (а), схема КО при C=0 (б), схема КО при C=1 (в)

Конфигурация схемы осуществляется значением C. При C=0 элемент X0 начинает выполнять роль логического буфера-повторителя B0, а элемент X1 – логического инвертора N0 (рис. 2.б). Для случая C=1 происходит обратная конфигурация: элемент X0 выполняет роль инвертора N1, а X1 – буфера-повторителя B1 (рис. 2.в). В обоих случаях кольцевая

схема содержит один инвертор, который обеспечивает генерацию периодического сигнала на выходе Q.

Данная схема может быть расширена на большее нечетное число n линий конфигураций C, которые в терминах ФНФ являются запросами, а ответами могут служить значения частот (периодов) вырабатываемых сигналов на выходе Q, либо однобитный ответ как результат сравнения двух частот, полученных различными значениями запроса. Для представленной схемы используются два элемента XOR2, а в общем случае число структурных элементов ККО выражается как $2n$. При этом n элементов XOR2 будут принимать на свои входы прямые значения бита запроса C_i, $i \in \{0, n\text{-}1\}$, а оставшаяся часть n элементов XOR2 – инверсные значения C_i. Подобная конфигурация обеспечит для произвольного значения запроса C наличие нечетного числа элементов XOR2 в схеме, что является необходимым условием функционирования кольцевых осцилляторов. Таким образом, представленная схема лишена недостатка схемы PD_4, для которой необходима дополнительная корректирующая аппаратура.

В свою очередь представленная схема ККО способна вырабатывать периодические сигналы с 2^n уникальными частотами, которая может быть классифицирована как сильная ФНФ и быть применена как для задач неклонируемой идентификации, так и для генерирования случайных чисел.

Покажем на примере простейшей схемы для n=1, что частота генерируемого сигнала F_Q зависит как от значения запроса C, так и от конфигурации ее межсоединений, и является уникальной при реализации схемы ККО. Для подтверждения этого тезиса рассмотрим временную модель предложенной схемы ККО и осуществим ее реализацию на ПЛИС типа FPGA.

3. Временная модель ККО

Частота генерируемого сигнала F есть величина обратная периоду P, определяемому как время, прошедшее от одного фронта сигнала (переднего фронта LH либо заднего фронта HL) до следующего аналогичного фронта на выходе Q. С учетом периодичности сигнала значение его периода можно представить как $P=P_L+P_H$, где P_L – время удержания сигнала в значении 0, а P_H – время удержания сигнала в значении 1. В идеализированном случае $P_L=P_H$, с практической точки зрения покажем, что это не так.

Значение P_L можно оценить как время, прошедшее от HL фронта сигнала до следующего во времени фронта LH: $P_L = t_{HL} - t_{LH}$. Аналогичным образом значение P_H можно оценить как $P_H = t_{LH} - t_{HL}$. Оба приведенных значения P_L и P_H зависят от задержек распространения сигнала в схеме, которые представлены транспортными задержками на линиях, соединяющих два элемента $X0$ и $X1$, и инерциальными задержками самих элементов XOR2.

Как было показано в работе [9] для двухвходового элемента XOR2 в режиме переключения сигнала по одному из его входов (Single Input Switching, SIS), приводящие к изменению сигнала на его выходе, можно выделить восемь уникальных значений задержек прохождения сигнала. В табл. 1 представлены формальные описания всех типов задержек для элемента XOR2 с входами a, b и выходом f в режиме SIS.

Таблица 1. Задержки сигнала на элементе XOR2

Задержка	*a*	*b*	*f*	Конфигурация	Задержка	*a*	*b*	*f*	Конфигурация
$\Delta_1(LH,0)$	*LH*	0	*LH*	буфер	$\Delta_5(HL,0)$	*HL*	0	*HL*	буфер
$\Delta_2(LH,1)$	*LH*	1	*HL*	инвертор	$\Delta_6(HL,1)$	*HL*	1	*LH*	инвертор
$\Delta_3(0,LH)$	0	*LH*	*LH*	буфер	$\Delta_7(0,HL)$	0	*HL*	*HL*	буфер
$\Delta_4(1,LH)$	1	*LH*	*HL*	инвертор	$\Delta_8(1,HL)$	1	*HL*	*LH*	инвертор

Например, приведенная в табл. 1 задержка $\Delta_4(1,LH)$ представляет собой задержку изменения сигнала на выходе *f* из 1 в 0 (*HL*) при изменении сигнала из 0 в 1 (*LH*) на входе *b* и удержании на входе *a* значения логической единицы. Для данной конфигурации элемента XOR2 (инвертор) с фиксированным значением сигнала на входе *a* имеется еще одна задержка $\Delta_8(1,HL)$ при изменении сигнала из 1 в 0 (*LH*) на входе *b*.

Представленные задержки являются уникальными и неповторимыми при реализациях схемы XOR2. С учетом этих задержек опишем временную модель схемы ККО (рис. 3). Условимся, что структурные элементы схемы подключены по одному из четырех возможны вариантов межсоединений. Конфигурационный сигнал *C* и его инверсное значение подключены к входам *a* схем *X*0 и *X*1: $C \to X0.a$, $\overline{C} \to X1.a$. Сами схемы соединены следующим образом: $X0.f \to X1.b$ и $X1.f \to X0.b$, транспортные задержки которых Δ^{P0} и Δ^{P1} не зависят от значений *C*.

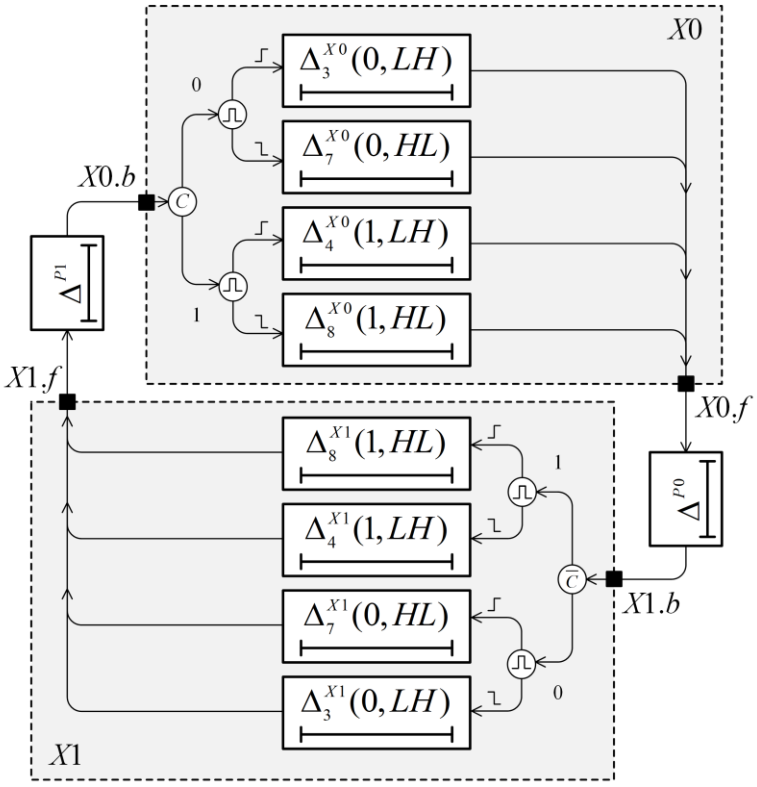


Рис. 3. Структура временной модели схемы ККО

Согласно приведенной модели рассмотрим значения P_L и P_H для двух конфигураций C=0 и C=1.

Пусть C=0, а на выходе $X0.f$ в начальный момент времени t_{HL} появляется спад *HL*, который с задержкой Δ^{P0} появится на входе $X1.b$. Инерциальная задержка элемента *X*1 в

конфигурации инвертора будет равна $\Delta_8^{X1}(1,HL)$. Далее, сформированный фронт сигнала *LH* на выходе *X*1.*f* с задержкой Δ^{P1} появится на входе *X*0.*b*. После прохождения элемента *X*0 в конфигурации буфера-повторителя фронт сигнала *LH* с задержкой $\Delta_3^{X0}(0,LH)$ в момент времени t_{LH} появится на выходе *X*0.*f*.

Таким образом, значение P_L при *C*=0 можно выразить следующей формулой:

$$P_L^{C=0} = t_{LH} - t_{HL} = \Delta^{P0} + \Delta_8^{X1}(1,HL) + \Delta^{P1} + \Delta_3^{X0}(0,LH). \quad (1)$$

Рассуждая аналогичным образом, можно показать, что значение P_H при *C*=0 будет равно:

$$P_H^{C=0} = t_{HL} - t_{LH} = \Delta^{P0} + \Delta_4^{X1}(1,LH) + \Delta^{P1} + \Delta_7^{X0}(0,HL). \quad (2)$$

В итоге $P_L^{C=0} \neq P_H^{C=0}$, что подтверждается ненулевым модулем их разности:

$$\left|P_L^{C=0} - P_H^{C=0}\right| = \left|\Delta_8^{X1}(1,HL) - \Delta_4^{X1}(1,LH)\right| + \left|\Delta_3^{X0}(0,LH) - \Delta_7^{X0}(0,HL)\right| \neq 0.$$

Тогда значение периода сигнала при *C*=0 выражается как сумма (1) и (2):

$$\begin{aligned} P^{C=0} &= P_L^{C=0} + P_H^{C=0} = \\ &= 2\cdot(\Delta^{P0} + \Delta^{P1}) + \Delta_8^{X1}(1,HL) + \Delta_3^{X0}(0,LH) + \Delta_4^{X1}(1,LH) + \Delta_7^{X0}(0,HL). \end{aligned} \quad (3)$$

При второй конфигурации схемы ККО (*C*=1) для элементов *X*0 и *X*1 будут применимы отличные от предыдущих значения задержек, а период генерируемого сигнала можно выразить следующей формулой:

$$P^{C=1} = 2\cdot(\Delta^{P0} + \Delta^{P1}) + \Delta_7^{X1}(0,HL) + \Delta_8^{X0}(1,HL) + \Delta_3^{X1}(0,LH) + \Delta_4^{X0}(1,LH). \quad (4)$$

Оценим модуль разницы значений двух периодов, представленных в формулах (3) и (4):

$$\begin{aligned} \Delta_P &= |P^{C=0} - P^{C=1}| = |\Delta_8^{X1}(1,HL) - \Delta_8^{X0}(1,HL)| + |\Delta_3^{X0}(0,LH) - \Delta_3^{X1}(0,LH)| + \\ &+ |\Delta_4^{X1}(1,LH) - \Delta_4^{X0}(1,LH)| + |\Delta_7^{X0}(0,HL) - \Delta_7^{X1}(0,HL)| \neq 0. \end{aligned} \quad (5)$$

С учетом уникальности представленных задержек в (5) для каждого реализованного элемента XOR2, периоды генерируемых сигналов, как и их частоты, не будут одинаковыми. Кроме этого, предположим, что ненулевая разница $\delta_i = \left|\Delta_i^{X0} - \Delta_i^{X1}\right|$, $i = \overline{1,8}$, между соответствующими задержками однотипных элементов гораздо меньше по модулю, чем разница между различными типами задержек этих же элементов $\delta_{ij} = \left|\Delta_i^{X0} - \Delta_j^{X1}\right|$, $\delta_{ij} \neq \delta_{ji}$, $\forall i \neq j,\ j = \overline{1,8}$: $\delta_i \ll \delta_{ij}$. При этом фактические значения δ_i и δ_{ij} являются случайными и неконтролируемыми для каждой реализации элементов XOR2.

Представленная модель описывает одну из четырех возможных конфигураций межсоединений схемы ККО для *n*=1, а именно для которой прямое значение сигнала *C* подается на вход *X*0.*a*, а обратное – на вход *X*1.*a*. В связи с этим обозначим данную модель *aa*, для которой используются следующие задержки (табл. 1): $\Delta_3(0,LH)$, $\Delta_4(1,LH)$, $\Delta_7(0,HL)$, $\Delta_8(1,HL)$. Остальные три конфигурации межсоединений схемы обозначим соответственно, как *ab*, *ba* и *bb*. В табл. 2 представлены типы задержек, которые используются для всех четырех приведенных конфигураций межсоединений схемы ККО.

Таблица 2. Используемые типы задержек

Конфигурация межсоединений ККО	Подключения	Типы используемых задержек
aa	$C \rightarrow X0.a$ $\bar{C} \rightarrow X1.a$	$\Delta_3(0,LH)$, $\Delta_4(1,LH)$, $\Delta_7(0,HL)$, $\Delta_8(1,HL)$
ab	$C \rightarrow X0.a$ $\bar{C} \rightarrow X1.b$	$\Delta_1(LH,0)$, $\Delta_2(LH,1)$, $\Delta_3(0,LH)$, $\Delta_4(1,LH)$, $\Delta_5(HL,0)$, $\Delta_6(HL,1)$, $\Delta_7(0,HL)$, $\Delta_8(1,HL)$
ba	$C \rightarrow X0.b$ $\bar{C} \rightarrow X1.a$	$\Delta_1(LH,0)$, $\Delta_2(LH,1)$, $\Delta_3(0,LH)$, $\Delta_4(1,LH)$, $\Delta_5(HL,0)$, $\Delta_6(HL,1)$, $\Delta_7(0,HL)$, $\Delta_8(1,HL)$
bb	$C \rightarrow X0.b$ $\bar{C} \rightarrow X1.b$	$\Delta_1(LH,0)$, $\Delta_2(LH,1)$, $\Delta_5(HL,0)$, $\Delta_6(HL,1)$

Для каждой конфигурации межсоединений определено 2^n уникальных частот вырабатываемых сигналов. Так, для рассматриваемого случая n=1 существует восемь уникальных частот на четырех конфигурациях межсоединений.

В терминах уникальных значений δ_i и δ_{ij} разницы в периодах (5) также будут уникальными для каждой конфигурации межсоединений схемы ККО. При этом для конфигураций *aa* и *bb* данные разницы будут принимать гораздо меньшие значения в сравнении с конфигурациями *ab* и *ba*. Выразим эти разницы через значения δ_i и δ_{ij} для всех конфигураций:

$$\begin{aligned}
\Delta_P^{aa} &= \delta_3 + \delta_4 + \delta_7 + \delta_8; \\
\Delta_P^{bb} &= \delta_1 + \delta_2 + \delta_5 + \delta_6; \\
\Delta_P^{ab} &= \delta_{24} + \delta_{31} + \delta_{68} + \delta_{75}; \\
\Delta_P^{ba} &= \delta_{13} + \delta_{42} + \delta_{57} + \delta_{86}.
\end{aligned} \qquad (6)$$

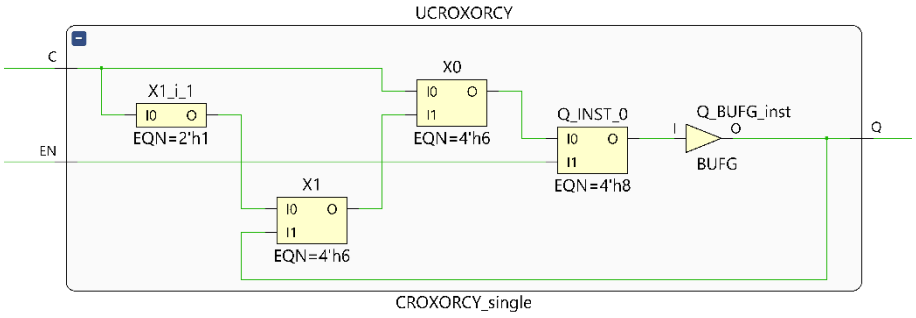
Таким образом, все представленные четыре разницы будут являться ненулевыми и уникальными, а реализованные схемы по четырем конфигурациям на одних и тех же элементах *X*0 и *X*1 будут генерировать периодические сигналы с различными восьмью частотами.

Для практического подтверждения описанных предположений проведем реализацию четырех конфигураций представленной схемы ККО на ПЛИС.

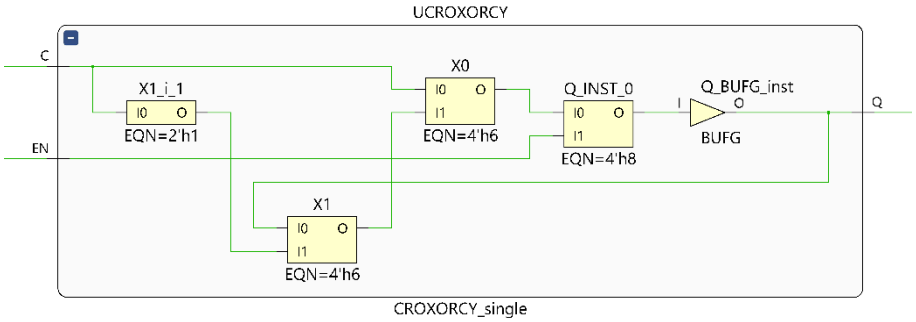
4. Исследование временных параметров ККО, реализованного на ПЛИС

Для реализации схемы ККО была выбраны две идентичные платы (B_0 и B_1) быстрого прототипирования цифровых систем Digilent ZYBO Z7-10 с ПЛИС типа FPGA Xilinx серии Zynq-7000 XC7Z010-1CLG400C, выполненной по 28 нм техпроцессу. Для проектирования использовался язык VHDL и САПР Vivado&Vitis 2020.2.

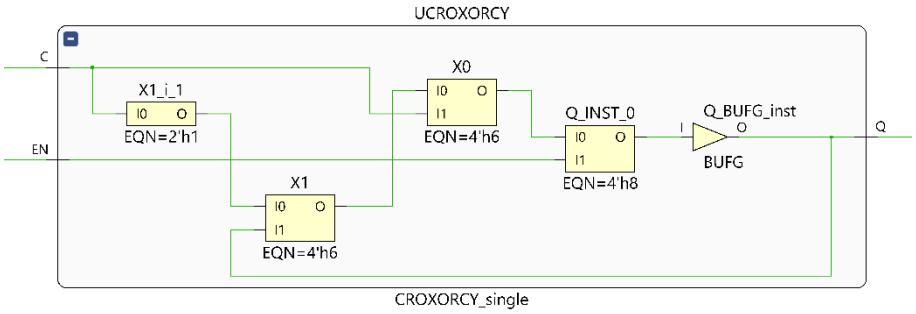
Элементы *X*0 и *X*1 исследуемой схемы ККО были реализованы на двух фиксированных блоках SLICEL_A5LUT и SLICEL_B5LUT, расположенных в логической части SLICE_X21Y52 CLB-блока соответственно.



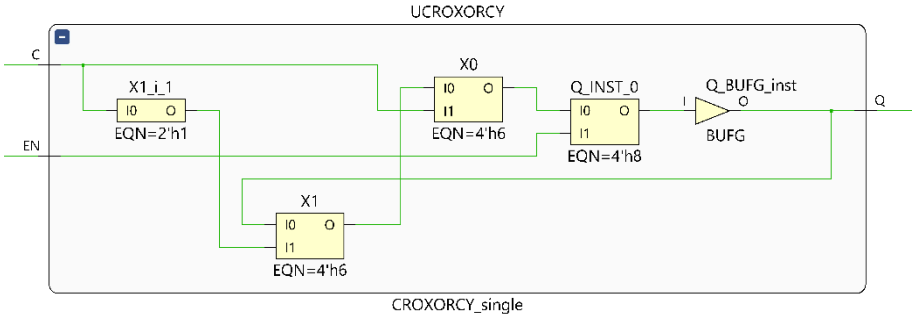
а)



б)



в)



г)

Рис. 4. Схема ККО в различных конфигурациях: aa (а), ab (б), ba (в), bb (г)

При этом, посредствам директивы `attribute lock_pins` были зафиксированы входы *a* и *b* элементов на конкретных физических входах I6 и I5 блоков SLICEL_A5LUT и SLICEL_B5LUT.

Для заданного фиксированного расположения элементов *X*0, *X*1 и их входов были получены четыре конфигурации ККО (рис. 4), которые исследовались на предмет оценки разницы в периодах, представленных в формуле (6). Для этого, дополнительно, было спроектировано цифровое устройство управления, позволяющее функционировать схеме ККО в заданном временном окне и проводить подсчет числа генерируемых импульсов на выходе *Q*.

Во всех проведенных экспериментах были использованы следующие параметры: системная таковая частота F_{SYS_CLK} = 50 МГц, временное окно измерения $TMW = 1/F_{SYS\_CLK} \times 10^6 = 20$ мс, количество повторяемых измерений E=100.

Для оценки значений периодов генерируемых сигналов был использован 32-разрядный двоичный счетчик, стробируемый сигналом с выхода *Q* схемы ККО, обеспечивающий подсчет количества N_{LH} фронтов *LH* в фиксированном временном интервале *TMW*. Тогда значение периода можно выразить как $P = TMW / N_{LH}$. В силу нестабильности значений N_{LH} оценим статистические характеристики измеряемых периодов на E повторяющихся экспериментах, а именно матожидание $\mu(P)$, среднеквадратическое отклонение $\sigma(P)$ и относительную девиацию $\sigma(P) / \mu(P)$.

В табл. 3 приведены перечисленные характеристики, в зависимости от значения *C*, конфигурации межсоединений схемы ККО, и реализации на плате B_0 либо B_1. Следует отметить, что программирование ПЛИС для двух плат осуществлялось одним и тем же BIT-образом, полученным в ходе технологического синтеза каждой схемной конфигурации.

Таблица 3. Статистические характеристики значений периодов сигналов для различных конфигураций межсоединений схем ККО, реализованных на двух платах B_0 и B_1

Плата	Характеристика	Конфигурация межсоединений							
		aa		*ab*		*ba*		*bb*	
		C=0	*C*=1	*C*=0	*C*=1	*C*=0	*C*=1	*C*=0	*C*=1
B_0	$\mu(P)$, нс	4,824	4,822	4,914	4,948	5,076	5,054	5,161	5,174
	$\sigma(P)$, пс	0,690	0,447	0,631	0,429	0,730	0,493	0,411	0,680
	$\sigma(P) / \mu(P)$, %	0,014	0,009	0,013	0,009	0,014	0,010	0,008	0,013
B_1	$\mu(P)$, нс	4,483	4,482	4,542	4,575	4,713	4,692	4,772	4,783
	$\sigma(P)$, пс	0,377	0,487	0,410	0,363	0,576	0,411	0,388	0,562
	$\sigma(P) / \mu(P)$, %	0,008	0,011	0,009	0,008	0,012	0,009	0,008	0,012

Как видно из представленных данных, все 16 реализованных конфигураций схемы ККО обладают уникальными значениями периодов генерируемых сигналов в диапазоне от 4,482 нс до 5,174 нс. При этом относительная девиация не превышает значения 0,014% (0,730 пс).

Согласно (6) значения разницы периодов конкретной реализации схемы ККО в зависимости от значения *C* также являются уникальными как в случае реализации на одном кристалле, так и на различных кристаллах. На рис. 5 представлена гистограмма значений Δ_P (5) для различных конфигураций и кристаллов ПЛИС.

Как и предполагалось аналитически, Δ_p^{ab} и Δ_P^{ba} являются бóльшими по абсолютным значениям в сравнении со значениями Δ_p^{aa} и Δ_P^{bb} в силу того, что включают в себя большее

число различных по типу и значениям задержек распространения сигнала структурных элементов схемы ККО (табл. 2). Ширина диапазона межкристальной разницы представленных значений составляет 2,347 пс, а ширина диапазона внутрикристальной разницы в зависимости от конфигурации – 31,466 пс и 31,932 пс для двух ПЛИС соответственно.

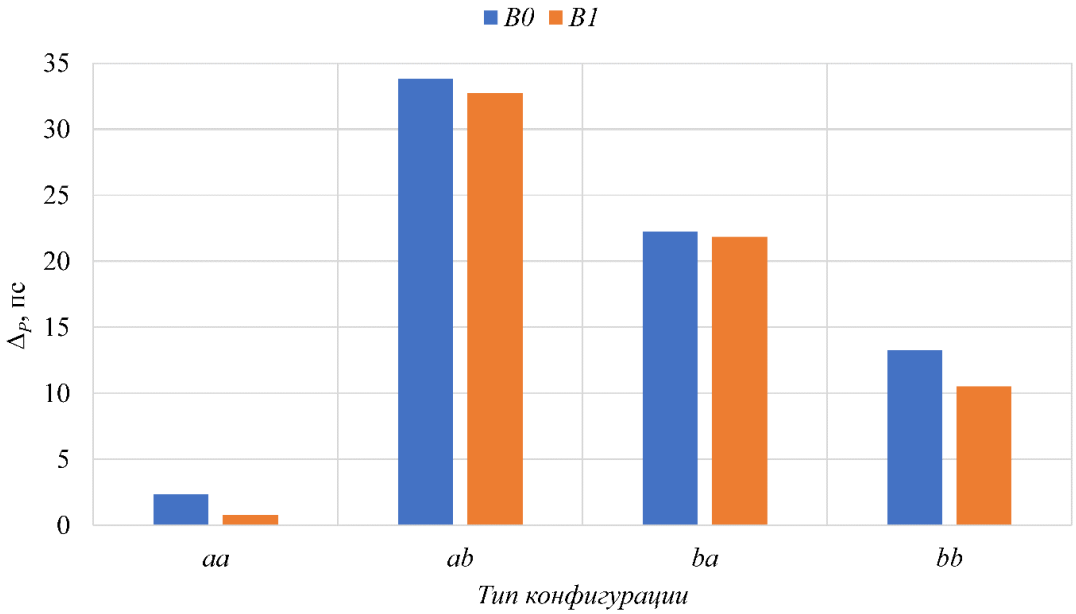
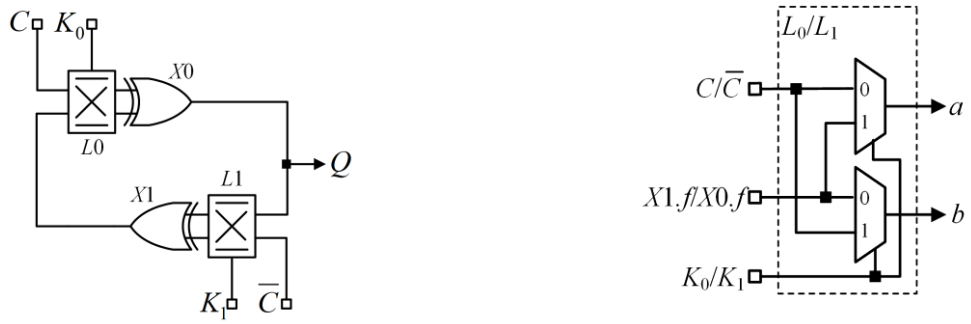


Рис. 5. Значения Δ_P для различных конфигураций и реализаций ККО

Для возможности задавать различные конфигурации межсоединений структурных элементов схемы ККО предлагается добавить коммутирующие элементы на подобие звеньев из классической схемы ФНФ типа арбитр [1]. На рис. 6.а приведена модифицированная схема ККО с возможностью задавать два вида конфигурации: конфигурацию подключения к входам элементов XOR2 (значениями K_0 и K_1) и конфигурацию самого ККО (значением запроса C).



а) *б*)

Рис. 6. Модифицированная схема ККО (а), схема коммутирующего элемента (б)

Коммутирующий элемент может быть реализован на двух мультиплексорах MUX2x1, как это показано на рис. 6.б. Он позволяет задавать как прямую, так и перекрестную коммутацию своих двух входов с двумя выходами. Наличие подобных элементов (L_0/L_1) обеспечивает задание произвольной конфигурации из четырех

возможных (*aa*, *ab*, *ba*, *bb*) при помощи установки соответствующих значений на входах K_0 и K_1.

Кроме этого, для каждой выбранной конфигурации возможно задание значения *C*, которое определяет функциональное назначение элементов *X*0 и *X*1. В итоге, модифицированная схема ККО позволяет вырабатывать сигналы на выходе *Q* с восемью уникальными частотами.

Рассмотренную схему ККО для n=1 можно линейно расширять, используя нечетные значения n, для которых возможна генерация выходного сигнала с уникальными 2^n частотами на каждой из 2^{2n} конфигураций межсоединений.

Другой подход к расширению схемы может заключаться в применении двух (n+1)-входовых элементов XOR и соответствующих коммутационных элементов [10], обеспечивающих в минимальном пределе $2^{\lfloor \log_2 (n+1)! \rfloor + 1}$ различных конфигураций межсоединений. Например, подобный подход позволяет применить два LUT6 технологических блока кристалла FPGA для реализации элементов XOR с параметром n=5 и 1024 различными конфирурациями их межсоединений.

Заключение

В статье представлена новая схема конфигурируемого кольцевого осциллятора, которая может быть использована в качестве основы для построения схем сильных ФНФ, пригодных для реализации задач неклонируемой идентификации и генерирования случайных чисел. Было показано, что для n-разрядного запроса предложенная схема способна вырабатывать выходные сигналы с 2^n уникальными частотами. Важную роль при этом играет конфигурация межсоединений структурных элементов ККО, мощность множества которых оценивается как 2^{2n}, что открывает новые возможности для построения ФНФ с улучшенными характеристиками случайности и уникальности. Работоспособность предложенной схемы была показана на примере ее реализации на ПЛИС типа FPGA.

СПИСОК ЛИТЕРАТУРЫ:

1. Ярмолик В.Н., Вашинко Ю.Г. Физически неклонируемые функции. Информатика. 2011, т. 30, № 2, с. 92–103. – EDN RBYGUD.
2. 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.
3. Иванюк А.А., Ярмолик В.Н. Физически неклонируемые функции на базе управляемого кольцевого осциллятора. Безопасность информационных технологий, [S.l.], т. 30, № 3, с. 90–103, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.3.06. – EDN: PWAZVG.
4. 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.
5. Zhang, Y., Li, J., Cheng, H., Zha, H., Draper, J. and Beerel, P.A. Yield modelling and analysis of bundled data and ring-oscillator based designs. IET Comput. Digit. Tech. 2019, v. 13, iss. 3, p. 262–272. DOI: https://doi.org/10.1049/iet-cdt.2018.5040.
6. Иванюк А.А. Применение конфигурируемых генераторов импульсов для идентификации ПЛИС. Информатика. 2011, т. 32, № 4, с. 113–123. URL: https://inf.grid.by/jour/article/view/343 (дата обращения: 11.04.2024).
7. Mahalat M. H., Ugale N., Shahare R. and Sen B. Design of Latch based Configurable Ring Oscillator PUF Targeting Secure FPGA. IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Verona, Italy. 2018, p. 261–266. DOI: 10.1109/VLSI-SoC.2018.8644737.
8. Kareem H., Dunaev D. A robust architecture of ring oscillator PUF: Enhancing cryptographic security with configurability. Microelectronics Journal. 2024, v. 143, 106002, с. 1–9. ISSN 0026-2692. DOI: https://doi.org/10.1016/j.mejo.2023.106022.

9. 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/10.37661/1816-0301-2021-19-1-32-49.
10. Иванюк А.А., Шамына А.Ю. Физически неклонируемая функция типа АБИТР с нелинейными парами путей. Системный анализ и прикладная информатика. 2023, №1, с. 54–62. DOI: https://doi.org/10.21122/2309-4923-2023-1-54-62.

REFERENCES:

[1] Yarmolik V.N., Vashinko Y.G. Physical unclonable functions. Informatics. 2011, v. 30, no. 2, p. 92–103 (in Russian). – EDN RBYGUD.
[2] 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.
[3] Ivaniuk A.A., Yarmolik V.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. DOI: http://dx.doi.org/10.26583/bit.2023.3.06 (in Russian). – EDN: PWAZVG.
[4] 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.
[5] Zhang, Y., Li, J., Cheng, H., Zha, H., Draper, J. and Beerel, P.A. Yield modelling and analysis of bundled data and ring-oscillator based designs. IET Comput. Digit. Tech. 2019, v. 13, no. 3, p. 262–272. DOI: https://doi.org/10.1049/iet-cdt.2018.5040.
[6] Ivaniuk A.A. Application of configurable pulse generator for FPGA identification. Informatics. 2011, v. 32, no. 4, p. 113–123 URL: https://inf.grid.by/jour/article/view/343 (accessed: 11.04.2024) (in Russian).
[7] Mahalat M. H., Ugale N., Shahare R. and Sen B. Design of Latch based Configurable Ring Oscillator PUF Targeting Secure FPGA. IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Verona, Italy. 2018, p. 261–266. DOI: 10.1109/VLSI-SoC.2018.8644737.
[8] Kareem H., Dunaev D. A robust architecture of ring oscillator PUF: Enhancing cryptographic security with configurability. Microelectronics Journal. 2024, v. 143, 106002, p. 1–9. ISSN 0026-2692. DOI: https://doi.org/10.1016/j.mejo.2023.106022.
[9] 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).
[10] Ivaniuk A.A., Shamyna A.Y. Physically non-cloneable arbiter-type function with non-linear path pairs. System analysis and applied information science. 2023, no. 1, p. 54–62 DOI: https://doi.org/10.21122/2309-4923-2023-1-54-62 (in Russian).

Поступила в редакцию – 15 апреля 2024 г. Окончательный вариант – 24 мая 2024 г.
Received – April 15, 2024. The final version – May 24, 2024.