Научная статья
УДК 004.056: 621.391
DOI: 10.26583/bit.2025.4.03

РЕАЛИЗАЦИЯ СИММЕТРИЧНЫХ ПУТЕЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ КОНФИГУРИРУЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА НА FPGA

Александр А. Иванюк[1], Ксена И. Трубач[2]
Белорусский государственный университет информатики и радиоэлектроники, ул. П. Бровки, 6, Минск, 220013, Беларусь
[1]ivaniuk@bsuir.by, https://orcid.org/0000-0002-6541-7742
[2]xenona11x@gmail.com, https://orcid.org/0009-0007-9626-3428

Аннотация. В статье предлагается новая схема физически неклонируемой функции (ФНФ), основанная на конфигурируемом кольцевом осцилляторе. Схема использует измерение разницы задержек распространения сигналов по симметричным путям, построенным на внутренних ресурсах LUT-блоков программируемых логических интегральных схем (ПЛИС) типа FPGA. Как было показано ранее, реализация строго симметричных путей на основе конфигурируемых соединений FPGA недостижима из-за априорного неравенства статических составляющих их задержек. Это положительно влияет на единообразие и внутрикристальную уникальность, но негативно сказывается на межкристальной уникальности ФНФ. Внутренняя структура LUT-блоков, функциональную основу которых составляет многовходовой мультиплексор, обладает большей степенью регулярности. Это позволяет использовать LUT-блоки для построения разнообразных ФНФ-схем с симметричными путями. Для предложенной схемы приведены основные параметры кольцевых осцилляторов и характеристики ФНФ, полученные как при моделировании, так и в ходе экспериментов с реализацией на кристаллах FPGA серии Xilinx ZYNQ 7000. Приемлемые показатели единообразия, стабильности, надежности, внутри- и межкристальной уникальности позволяют рассматривать предложенную схему в качестве кандидата для проектирования средств уникальной идентификации и защиты от клонирования цифровых устройств. Для автоматизации и обеспечения достоверности экспериментов было разработано специализированное микропрограммное ядро управления ФНФ-схемами. Помимо автоматизации экспериментов и расчета характеристик, данное ядро может быть использовано на практике для реализации процедур неклонируемой идентификации, аутентификации и генерации случайных данных.

Ключевые слова: *физически неклонируемые функции, конфигурируемый кольцевой осциллятор, симметричные пути, межкристальная уникальность.*

Для цитирования: *Иванюк, Александр А.; Трубач, Ксена И. Реализация симметричных путей физически неклонируемой функции конфигурируемого кольцевого осциллятора на FPGA. Безопасность информационных технологий, [S.l.], т. 32, № 4, с. 37–51, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1865. DOI: https://doi.org/10.26583/bit.2025.4.03.*

Scientific article

IMPLEMENTATION OF CONFIGURABLE RING OSCILLATOR PUF WITH SYMMETRICAL PATHS ON FPGA

Alexander A. Ivaniuk[1], Ksena I. Trubach[2]
Belarusian State University of Informatics and Radioelectronics, P. Brovki St., 6, Minsk, 220013, Belarus
[1]ivaniuk@bsuir.by, https://orcid.org/0000-0002-6541-7742
[2]xenona11x@gmail.com, https://orcid.org/0009-0007-9626-3428

Abstract. This paper proposes a novel Physical Unclonable Function (PUF) scheme based on a configurable ring oscillator. The circuit utilizes the measurement of signal propagation delay differences along symmetric paths constructed using the internal resources of Look-Up Table (LUT) blocks within Field-Programmable Gate Array (FPGA) integrated circuits. As previously demonstrated, achieving strictly symmetric paths via FPGA configurable interconnects is unattainable due to the inherent inequality of their static delay components. This phenomenon positively impacts uniformity and intra-die uniqueness but adversely affects the PUF's inter-die uniqueness. The internal structure of LUT blocks, whose functional core is a multi-input multiplexer, exhibits a higher degree of regularity. This enables the use of LUT blocks for constructing diverse PUF circuits with symmetric paths. For the proposed scheme, the core parameters of the ring oscillators and the PUF characteristics, obtained through both simulation and experimental implementation on Xilinx ZYNQ 7000 series FPGA devices, are presented. The acceptable metrics for uniformity, stability, reliability, intra, and inter-die uniqueness position the proposed circuit as a candidate for designing solutions for unique identification and anti-cloning of digital devices. To automate and ensure the reliability of the experiments, a specialized microprogrammed core for managing PUF circuits was developed. Beyond automating experiments and calculating characteristics, this core can be utilized in practice to implement procedures for unclonable identification, authentication, and random data generation.

Keywords: *physical unclonable functions, configurable ring oscillator, symmetrical paths, inter-chip uniqueness.*

For citation: *Ivaniuk, Alexander A.; Trubach, Ksena I. Implementation of configurable ring oscillator PUF with symmetrical paths on FPGA. IT Security (Russia), [S.l.], v. 32, no. 4, p. 37–51, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1865. DOI: https://doi.org/10.26583/bit.2025.4.03.*

Введение

Помимо традиционных и хорошо зарекомендовавших себя методов защиты интеллектуальной собственности от нелегального использования и копирования, большинство которых было разработано для программного обеспечения, развиваются и находят свое применение методы физической криптографии, в основе которых лежат физически неклонируемые функции (ФНФ), основанные на извлечении уникальных физических параметров реализованных цифровых устройств. По сути, ФНФ представляет собой специальную цифровую схему, которую легко спроектировать и реализовать, но практически невозможно воспроизвести [1]. Среди всего многообразия ФНФ выделяют схемы, основанные на оценке задержек распространения сигналов. К подобным типам ФНФ можно отнести ФНФ типа арбитр (АФНФ) [2] и ФНФ кольцевых осцилляторов (ФНФ КО) [3–7].

В [8] предложен подход к построению модели, обобщающей этот класс ФНФ и основанной на сравнении задержек распространения сигнала в парах из множества конфигурируемых симметричных путей. В [9] определен набор метрик, позволяющих оценить приемлемость ФНФ для описанных ранее задач, и показано, что предложенная модель демонстрирует достаточные уровни единообразия (*UNF*, *Uniformity*), внутрикристальной уникальности (UNQ^{ra}, *Intra-die Uniqueness*), стабильности (*STA*, *Stability*) и надёжности (*REL*, *Reliability*), но обладает недостатком в виде неприемлемо низкого уровня межкристальной уникальности (UNQ^{er}, *Inter-die Uniqueness*). Это серьёзно ограничивает потенциал использования такой схемы для задач идентификации.

Настоящая статья ставит своей задачей спроектировать модель, которая была бы лишена ранее описанных недостатков. Проводится качественная оценка модели и сравнение с характеристиками ранее предложенной модели [8]. Показано, что симметрия схемы значительно возросла и более чем в 10 раз улучшила метрику межкристальной

уникальности UNQ^{er}, однако несколько снизила метрики стабильности *STA* и надёжности *REL*.

Для решения задач неклонируемой идентификации [10, 11] исследователи и разработчики схем ФНФ стремятся достичь максимальных значений перечисленных характеристик, а для схем генерирования случайных числовых последовательностей [12] – нулевых значений надежности *REL* и стабильности *STA*. В современных работах описываются методы, позволяющие повысить значение уникальности. Такими примерами могут служить: модификация базовых элементов ФНФ [13], искусственное балансирование путей для ФНФ типа «арбитр» с применением программируемых линий задержек [14] и т.д. Для повышения иных характеристик применяются различные методы постобработки [15, 16]. Тем не менее, одним из важнейших критериев, влияющих на характеристики ФНФ, является симметрия путей [17].

Рассмотрим подробнее, как симметрия путей влияет на задержку распространения сигналов и значения ответов ФНФ. Если пара путей заведомо является асимметричной, то на различных копиях схемы может наблюдаться одинаковое постоянное значение ответа *R* для выбранного запроса, что негативно скажется на характеристике межкристальной уникальности UNQ^{er}. Поэтому обеспечение симметрии путей является определяющей задачей при построении схем ФНФ с высокими значениями их характеристик. При этом, если построение ФНФ ведётся на базе технологий ASIC, то обеспечение симметрии конфигурируемых путей возможно, в отличие от ПЛИС, где такая реализация затруднена. Соединения, задействованные в конкретной схеме на ПЛИС, асимметричны по своей природе [18]. Такое свойство крайне положительно сказывается на метрике внутрикристальной уникальности UNQ^{ra}, поскольку все пути внутри одного кристалла различны, однако приводит к недостаточным уровням межкристальной уникальности UNQ^{er} при сравнении на наборе ПЛИС. Что примечательно, технология ASIC не обладает такой особенностью, и при её использовании показатели межкристальной и внутрикристальной уникальности сравнимы между собой $UNQ^{er} \approx UNQ^{er}$. Отсюда, если рассмотреть ПЛИС, например, типа FPGA, как полупроводниковый кристалл, выполненный по технологии ASIC, пути в котором реализуются посредством конфигурируемых связей, имеющих заведомую физическую асимметрию [17], то можно заметить, что LUT-блоки, функционально представляющие собой каскад мультиплексоров, внутри симметричны. Используя это свойство, можно получить схему, которая значительно приблизит получаемые значения межкристальной уникальности к приемлемым (по сравнению со схемой, представленной в [8]).

Проведенные исследования в [8] схем ФНФ конфигурируемых КО показывают следующие результаты для ПЛИС типа FPGA Xilinx Zynq 7000 (табл. 1), которые подтверждают сделанные ранее выводы.

Таблица 1. Значения основных характеристик ФНФ ККО

$\sigma \cdot \mu^{-1}$, %		*REL*		*STA*		*UNF*		UNQ_k^{ra}		UNQ_k^{er}	
min	max	min	max	min	max	min	max	min	max	min	max
10,4	13,6	0,9853	0,9986	0,9989	0,9993	0,9908	0,9998	0,1124	0,3922	0,0074	0,0145

Минимальные и максимальные значения характеристик, представленные в табл. 1, соответствуют различным стратегиям размещения путей на кристаллах. Так, автоматическая стратегия размещения дает большую асимметрию, выраженную показателем $\sigma\ \mu^{-1}$ равным 13,6%. При ручном размещении компонент путей ФНФ удалось снизить этот показатель до 10,4% и почти в два раза увеличить межкристальную

уникальность UNQ_k^{ra} (параметр k определяет число сравниваемых компонент [8]). Однако сами значения характеристики UNQ_k^{er} в обоих стратегиях размещения являются неприемлемыми на практике. Как и предполагалось, большая асимметрия путей дала высокие показатели характеристик надежности, стабильности и единообразия, вне зависимости от стратегии размещения.

В данной статье предлагается новый подход для увеличения симметрии путей схем ФНФ ККО, реализуемых на ПЛИС типа FPGA.

1. Предлагаемая схема симметричных путей ФНФ ККО

На рис. 1 представлены фрагменты обобщенных структур симметричных путей ФНФ ККО, реализованных на ресурсах блоков LUT и конфигурируемых межсоединениях.

В реализованной и исследованной ранее схеме ФНФ ККО [8] на блоках LUT размещались мультиплексоры в конфигурации 4x1, а фрагменты путей представляли собой четыре программируемые линии межсоединений, связывающие выход одного LUT-блока с четырьмя входами смежного LUT-блока (рис. 1.а).

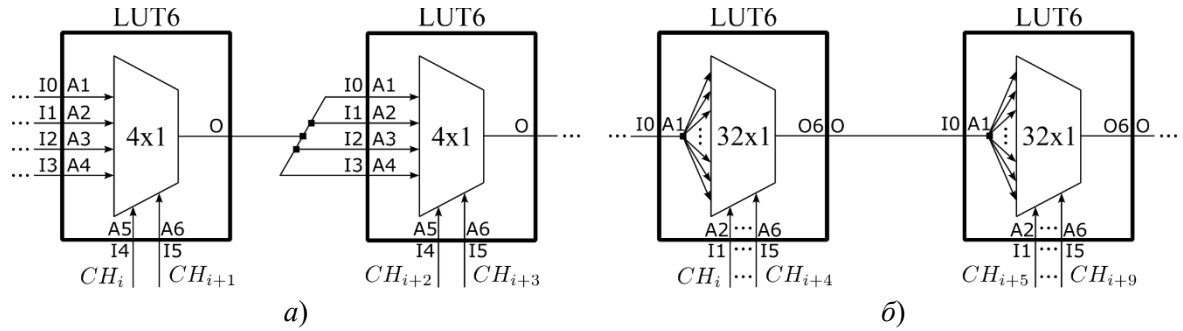

Рис. 1. Фрагменты схем симметричных путей ФНФ ККО: ранее исследованная схема (а), предлагаемая схема (б)

Для нивелирования большой асимметрии межсоединений предлагается путем соответствующих конфигураций в блоках LUT6 реализовать мультиплексоры в конфигурации 32x1, при которой множественные копии одного входного сигнала будут коммутироваться с выходом O (см. рис. 1.б). При этом все 32 фрагмента путей, реализованных на одном блоке LUT, будут максимально идентичны в силу симметричности каскадной схемы внутренних мультиплексоров. Для увеличения протяженности внутренних путей для тестового сигнала от входа I0 блока LUT до его выхода необходимо его привязать к физическому младшему адресному входу A1, что выполняется соответствующей директивой LOC_PINS в исходном коде проекта на языке VHDL:

```
attribute LOCK_PINS : string;
attribute LOCK_PINS of L0 : label is
"I0:A1, I1:A2, I2:A3, I3:A4, I4:A5, I5:A6";
```

Оставшиеся пять входов блока LUT будут выполнять роль селективных сигналов, которые определяют один из 32 возможных путей распространения входного сигнала. Ниже представлено структурное описание такого элемента L0 (см. рис. 2), где сигнал s(0) является межсоединением с последующим блоком L1, сигнал fb – обратная связь от последнего элемента схемы СККО, C(0) – C(4) – разряды шины конфигурации:

```
L0: LUT6 generic map ( X"AAAAAAAAAAAAAAAA" )
port map (
O  => s( 0 ),
I0 => fb,
I1 => C( 0 ),
I2 => C( 1 ),
I3 => C( 2 ),
I4 => C( 3 ),
I5 => C( 4 ) );
```

Для корректной реализации сигнал fb требует следующие директивы:

```
attribute DONT_TOUCH : string;
attribute DONT_TOUCH of fb: signal is "yes";
attribute ALLOW_COMBINATORIAL_LOOPS : string;
attribute ALLOW_COMBINATORIAL_LOOPS of fb : signal is "TRUE";
```

Следующим образом фиксируется расположение структурного элемента L0 в младшем (A) LUT-блоке логической части CLB-блока (SLICEL) и координатах (XL0,YL0) SLICE части блока CLB:

```
attribute BEL : string;
attribute BEL of L0: label is "SLICEL_A6LUT";
attribute LOC : string;
attribute LOC of L0: label is
"SLICE_X" & integer'image( XL0 ) & "Y" & integer'image( YL0 );
```

Подобного рода реализация должна уменьшить параметр $\sigma\,\mu^{-1}$ и сделать схожими характеристики UNQ_k^{ra} и UNQ_k^{er}. При этом уменьшение СКО периодов осцилляторов приведет к увеличению числа метастабильных ответов в сравнении с ранее исследованными схемами ФНФ ККО.

Схема ФНФ ККО, построенная по предложенному принципу реализации симметричных путей, будет основана на сравнении задержек распространения сигналов не по протяженным асимметричным линиям межсоединений FPGA, а по симметричным фрагментам внутренних линий LUT-блоков. Если для предыдущей схемы применение K блоков LUT6 дает возможность реализовать схему ФНФ с мощностью множества запрос-ответ CHR равным 2^{2K}, то для предложенной схемы $|CHR| = 2^{5K}$.

На рис. 2 представлена схема ККО с симметричными конфигурируемыми путями (СККО), реализованными на внутренних ресурсах LUT6 блоков для K=5, что является условием сравнения с ранее исследованной схемой [8]. Для обоих типов схем было выбрано число симметричных путей $M=2^{10}$, а разрядность шины запроса n=20.

С учетом того, что при формировании ответа R значение задержки распространения сигнала по общей программируемой линии межсоединений LUT-блоков не будет учитываться, то сценарий их размещения на кристалле не будет оказывать существенное влияние на основные характеристики схемы.

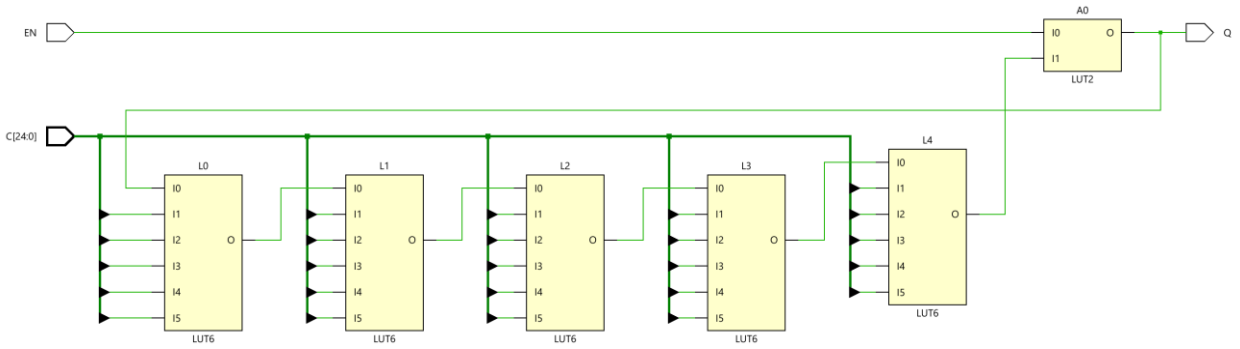

Рис. 2. Предлагаемая схема СККО для K=5

Как и для предыдущей схемы, для реализации были использованы те же четыре кристалла ПЛИС Xilinx ZYNQ 7000 ($FPGA_0$ – $FPGA_3$), на каждом из которых были реализованы четыре копии новой схемы СККО (CRO_0 – CRO_3).

В настоящей работе, в отличие от [8], представлено автоматизированное решение – узкоспециализированное микропрограммное ядро (рис. 3), предназначенное как для проведения исследований схем ФНФ, так и для их практического применения. Ядро, по сути, является системой управления ФНФ и обеспечивает реализацию таких функций, как неклонируемая идентификация, аутентификация и генерация случайных чисел. Ядро основано на микроархитектуре с регистровым файлом общего назначения (GPR), а архитектура набора инструкций (ISA) разработана с учётом принципов открытой архитектуры RISC-V[1]. Однако ISA включает исключительно те инструкции, которые необходимы для расчёта перечисленных ранее метрик (за исключением UNQ_k^{er}). В это множество входит выполнение арифметических операций, взаимодействие с памятью, а также специализированные инструкции для генерации запросов C_i и управления схемами ФНФ.

Для хранения микропрограммы предусмотрено постоянное перепрограммируемое запоминающее устройство (PROM). Загрузка инструкций в PROM и управление ядром осуществляются через интерфейсы UART и AXI4 Lite и регистровый файл (*RF, register file*), который универсализирует доступ к ядру (*MPCU, micro programmable control unit*). Оперативное запоминающее устройство логически разделяется на две части: одна (*general purpose RAM*) отводится под общие цели (вычисления, анализ и др.), вторая (*RAM Mapper PUF CSRs*) предназначена для работы с компонентами ФНФ (PUF_1, ..., PUF_n).

Функционирование любой ФНФ в паре с предложенным ядром требует использования как минимум двух ключевых параметров: запроса C и ответа R. В зависимости от типа ФНФ может также потребоваться набор дополнительных управляющих сигналов (инициализация и разрешение функционирования). С целью обеспечения расширяемости и масштабируемости системы для каждой ФНФ выделяется собственный регистровый блок, отображенный на память. Этот блок предназначен для хранения упомянутых параметров и других необходимых сигналов. При этом каждому типу ФНФ присваивается уникальный идентификатор, на основе которого ядро автоматически выбирает соответствующий алгоритм управления. Такой подход снижает сложность пользовательского микрокода, поскольку общие операции управления инкапсулированы непосредственно в аппаратной логике ядра и вызываются

[1]RISC-V Technical Specifications. RISC-V Tech Hub. URL: https://lf-riscv.atlassian.net/wiki/x/kYD2 (дата обращения: 30.06.2025).

специализированными инструкциями. Для генерации запросов в ядре присутствует отдельный блок (*CHG, Challenge generator*).

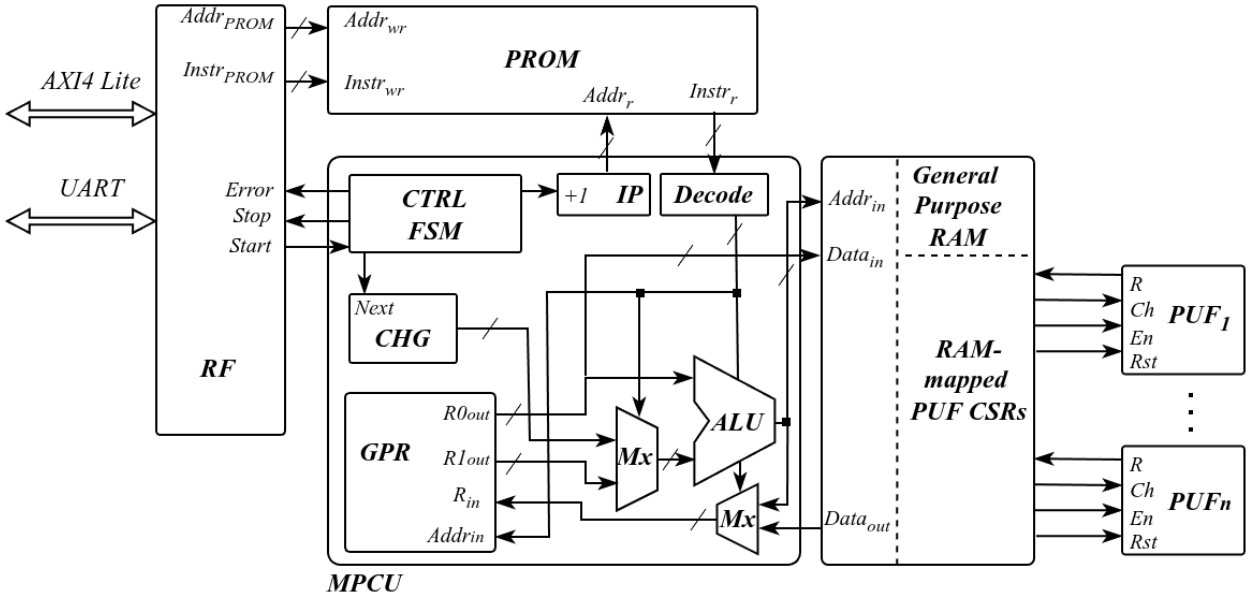

Рис. 3. Схема предлагаемого ядра автоматизации

Для оценки эффективности предложенного микропрограммного ядра в контексте управления ФНФ и расчёта их характеристик была проведена серия экспериментальных исследований на отладочной плате Zybo Z7, оснащённой ПЛИС Xilinx Zynq 7010[2] и функционирующей в среде PYNQ[3] под управлением Jupyter Notebook[4]. В качестве тестового примера рассматривался процесс вычисления внутрикристальной уникальности для двух физически неклонируемых функций (ФНФ), реализованных на ПЛИС, при количестве запросов $T = 64$. Сравнительному анализу подвергались два подхода к реализации расчёта: первый – с использованием языка Python, обеспечивающего доступ к ФНФ посредством регистрового файла, управляемого протоколом AXI4 Lite; второй – с использованием разработанного набора инструкций, исполняемых предложенным ядром. При этом запуск ядра и получение результатов также осуществлялись через вышеупомянутый регистровый файл. Каждый из экспериментов был проведён дважды: в условиях минимальной и максимальной загруженности процессорной системы Zynq. Полученные результаты продемонстрировали, что применение микропрограммного ядра обеспечивает ускорение выполнения кода более чем на два порядка. При этом в условиях высокой загрузки системы снижение производительности ядра составляет лишь 2,5%, в то время как аналогичный показатель для реализации на языке Python достигает 5%. Данный факт свидетельствует о снижении зависимости измерительной системы от влияния внешних факторов, в частности, от интенсивности использования процессорной системы,

[2]Zynq-7000 Soc Data Sheet: Overview (DS190). AMD. URL: https://docs.amd.com/v/u/en-US/ds190-Zynq-7000-Overview (дата обращения: 30.06.2025).
[3]PYNQ Introduction / PYNQ: Python productivity for Zynq. URL: https://pynq.readthedocs.io/en/latest/ (дата обращения: 30.06.2025).
[4]Project Jupyter Documentation. Jupyter Documentation 4.1.1 alpha documentation. URL: https://docs.jupyter.org/en/latest (дата обращения: 30.06.2025).

что, в свою очередь, положительно сказывается на временных характеристиках и достоверности получаемых результатов.

2. Исследование схемы ФНФ СККО

Рассмотрим модельные и реалистичные значения основных характеристик предложенной схемы в автоматическом (*Auto*) и фиксированном (*Fixed*) расположениях, которые были использованы ранее для предыдущей схемы [8]. Также следует отметить, что использованная САПР не позволяет модельно оценить задержки распространения сигналов от различных входов блоков LUT до их выходов, что приводит к одному и тому же значению периода при подаче различных запросов для выбранной схемы СККО. При этом влияние на значения периодов оказывает тип размещения компонент и выбранный сценарий моделирования (табл. 2).

Таблица 2. Значения периодов моделей СККО в различных сценариях моделирования и размещения

Тип размещения	СККО	Сценарий			
		Slow		*Fast*	
		Max	*Min*	*Max*	*Min*
Auto	CRO_0	13,352	11,02	5,84	4,86
	CRO_1	15,166	12,492	6,518	5,412
	CRO_2	14,242	11,774	6,228	5,206
	CRO_3	13,052	10,476	5,674	4,628
Fixed	CRO_0	12,154	9,974	5,058	4,168
	CRO_1	12,338	10,122	5,234	4,318
	CRO_2	12,254	10,064	5,074	4,184
	CRO_3	12,55	10,304	5,29	4,37

Как видно из табл. 2, меньшим разбросом значений периодов обладают модели схем с фиксированным размещением компонент и идентичными межсоединениями на технологических ресурсах ПЛИС. Как показали полученные данные от реальных схем ККО, значения их периодов близки, как и в случае предыдущих схем, к модельным оценкам в сценарии *Fast*/*Max* [8].

На рис. 4 приведены значения плотностей вероятностей реальных периодов четырех схем СККО, реализованных на одной ПЛИС ($FPGA_2$), и одной схемы СККО (CRO_0) на четырех различных кристаллах.

Как и предполагалось, асимметрия межсоединений FPGA наблюдается даже на модельных оценках периодов схем в различных типах размещения и сценариях моделирования. Наибольший разброс значений периодов наблюдается для схем в автоматическом размещении для сценария моделирования *Slow*/*Max*, а наименьший – в фиксированном размещении для сценария моделирования *Fast*/*Min*, и составляют 2,114 нс и 0,202 нс соответственно.

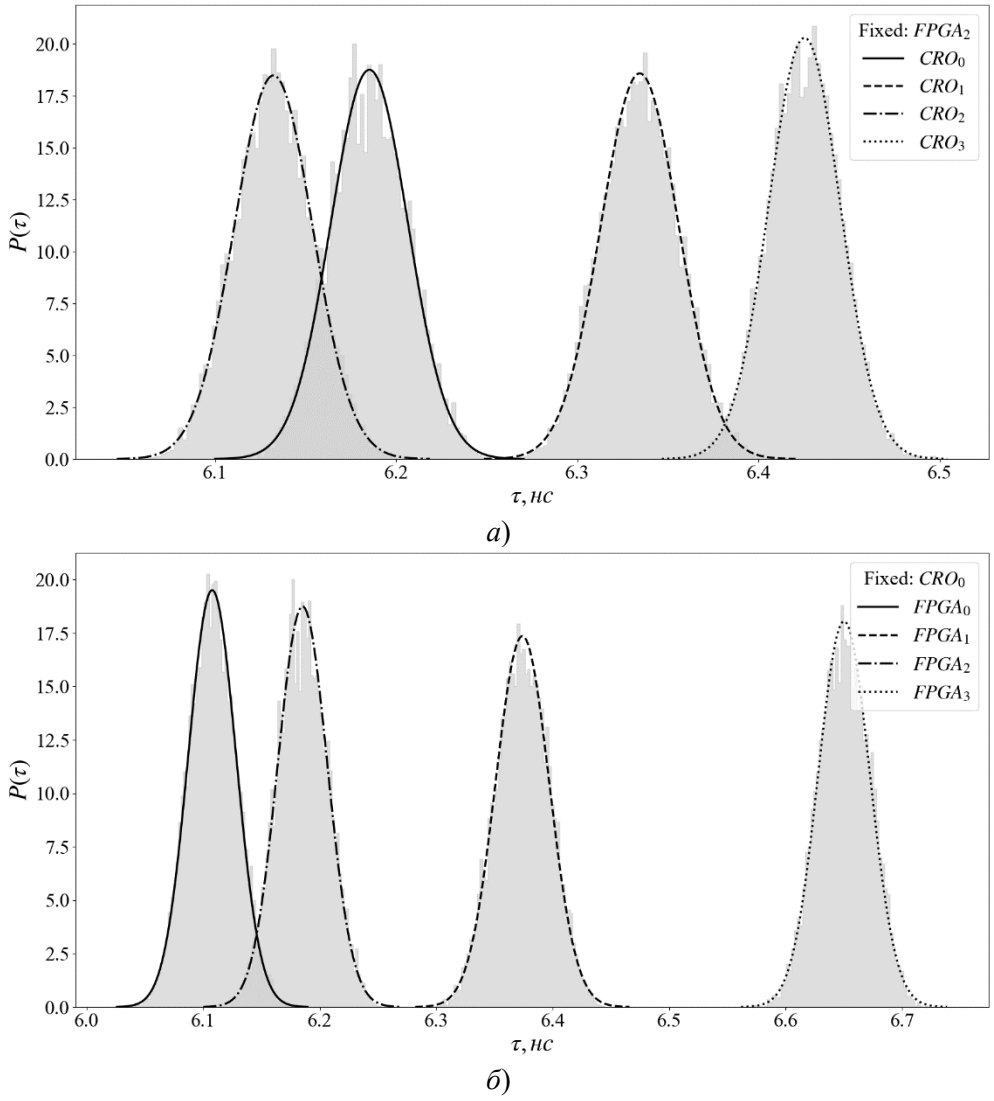

Рис. 4. Плотность вероятности периодов всех компонент, фиксированно размещенных на кристалле $FPGA_2$ (а) и для компоненты CRO_0, реализованной на различных ПЛИС (б)

Как видно из приведенных графиков, разброс значений периодов $\tau_i = 2\Delta_i$ для всех компонент мал в сравнении с рассмотренными ранее схемами, что говорит о большей степени симметрии конфигурируемых путей схем СККО. Кроме этого, наблюдается высокая уникальность периодов схем, реализованных на одном кристалле, так и на разных кристаллах, что потенциально может улучшить значения соответствующих характеристик ФНФ СККО.

В табл. 3 приведены характеристики периодов сигналов схем реальных схем СККО, полученных при автоматическом и фиксированном размещении. Значение среднеквадратического отклонения периодов в среднем составляет около 20 пс как при автоматическом, так и при фиксированном размещении и обусловлено в основном девиациями задержек на LUT-блоках.

Как было отмечено и при моделировании (см. табл. 2) значения ожидаемых периодов схем СККО отличаются как при реализации на одном кристалле FPGA, так и на различных кристаллах. Наибольший разброс между периодами наблюдается при

реализации схем на $FPGA_3$ с автоматическим размещением (1,075 нс), а наименьший – для $FPGA_1$ с фиксированным размещением (0,251 нс).

Таблица 3. Характеристики периодов сигналов реальных СККО в различных типах размещения на различных ПЛИС

ПЛИС	СККО	min(T), нс		max(T), нс		μ, нс		σ, нс		σ/μ, %	
		Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed
$FPGA_0$	CRO_0	6,936	6,037	7,063	6,177	6,995	6,108	0,020	0,020	0,291	0,335
	CRO_1	7,690	6,150	7,809	6,286	7,747	6,215	0,018	0,019	0,227	0,308
	CRO_2	7,189	6,018	7,308	6,153	7,249	6,085	0,018	0,022	0,249	0,354
	CRO_3	6,665	6,286	6,805	6,426	6,732	6,357	0,021	0,022	0,308	0,345
$FPGA_1$	CRO_0	7,226	6,299	7,353	6,444	7,288	6,374	0,019	0,023	0,263	0,361
	CRO_1	8,027	6,466	8,167	6,601	8,098	6,534	0,022	0,021	0,268	0,322
	CRO_2	7,546	6,301	7,666	6,445	7,605	6,382	0,017	0,020	0,226	0,313
	CRO_3	6,966	6,545	7,098	6,690	7,035	6,625	0,022	0,022	0,306	0,326
$FPGA_2$	CRO_0	6,999	6,123	7,140	6,253	7,067	6,185	0,021	0,021	0,299	0,344
	CRO_1	7,784	6,268	7,916	6,409	7,854	6,334	0,019	0,021	0,243	0,339
	CRO_2	7,277	6,056	7,394	6,206	7,337	6,132	0,017	0,022	0,235	0,352
	CRO_3	6,753	6,355	6,878	6,500	6,815	6,425	0,018	0,020	0,270	0,306
$FPGA_3$	CRO_0	7,607	6,572	7,744	6,722	7,678	6,650	0,022	0,022	0,282	0,332
	CRO_1	8,397	6,706	8,540	6,859	8,470	6,788	0,021	0,023	0,244	0,337
	CRO_2	7,890	6,602	8,054	6,735	7,959	6,666	0,020	0,018	0,254	0,277
	CRO_3	7,319	6,876	7,508	7,038	7,395	6,960	0,025	0,024	0,335	0,338

Высокая идентичность межсоединений при фиксированном типе размещения дает более близкие оценки матожидания и, соответственно, чуть большие значения удельного СКО $\sigma\ \mu^{-1}$, в сравнении с автоматическим типом, которые в среднем составляют 0,33%, в отличие от 11,22% для рассмотренных ранее схем ККО [8]. Также существенно, более чем в 20 раз, уменьшились диапазоны изменения периодов, средние значения которых составляют 136 пс и 143 пс для автоматического и фиксированного размещения соответственно.

В общем случае, приведённые в табл. 2 данные свидетельствуют о большей схожести схем – как тех, что реализованы внутри каждой FPGA, так и тех, что реализованы на различных кристаллах.

Рассмотрим, как приведенные характеристики периодов предложенной схемы СККО влияют на свойства схем ФНФ. В табл. 4 приведены значения характеристики *UNF*, которые мало зависят от типа применяемого размещения и в среднем составляют 0,9879 и 0,9894 при автоматическом и фиксированном размещении соответственно. В сравнении с приведенными ранее значениями *UNF* уменьшилось менее чем на 0,5%.

Таблица 4. Значения метрики единообразия UNF схем ФНФ СККО в различных типах размещения

ПЛИС	CRO_0		CRO_1		CRO_2		CRO_3	
	Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed
$FPGA_0$	0,9824	0,9902	0,9982	**0,9756**	0,9876	0,989	0,9866	0,996
$FPGA_1$	0,9828	0,983	0,9848	0,9932	0,9902	0,9834	0,9834	0,9944
$FPGA_2$	0,9822	0,9828	0,9904	0,989	0,9894	0,995	0,9862	0,992
$FPGA_3$	0,9942	0,9874	**1,0**	0,9896	0,9824	0,9984	0,9868	0,9922

Что касается метрик внутрикристальной и межкристальной уникальности (см. табл. 5 и 6), то их значения в среднем близки к значению 0,25 и не зависят от типа размещения.

Таблица 5. Значения метрик внутрикристальной уникальности схем ФНФ СККО

Размещение	ПЛИС	Внутрикристальная уникальность						
		$UNQ_{0,1}$	$UNQ_{0,2}$	$UNQ_{0,3}$	$UNQ_{1,2}$	$UNQ_{1,3}$	$UNQ_{2,3}$	UNQ_4^{ra}
Auto	$FPGA_0$	0,2761	0,2706	0,2333	0,2225	0,2606	0,2621	**0,2542**
	$FPGA_1$	0,2062	0,2793	0,2496	0,2911	0,2588	**0,3507**	**0,2726**
	$FPGA_2$	0,2437	0,2776	0,2591	0,2667	0,216	0,2945	**0,2596**
	$FPGA_3$	0,2518	0,2573	0,2642	0,2685	0,224	0,2479	**0,2523**
Fixed	$FPGA_0$	0,2468	0,2553	0,2235	0,2663	0,2605	0,2532	**0,2509**
	$FPGA_1$	**0,1944**	0,2155	0,2465	0,2277	0,2759	0,2396	**0,2333**
	$FPGA_2$	0,2314	0,2911	0,2631	0,2845	0,2519	0,288	**0,2683**
	$FPGA_3$	0,2656	0,2632	0,2787	0,2974	0,2907	0,2799	**0,2792**

Таблица 6. Значения метрик межкристальной уникальности схем ФНФ СККО

Размещение	СККО	Межкристальная уникальность						
		$UNQ_{0,1}$	$UNQ_{0,2}$	$UNQ_{0,3}$	$UNQ_{1,2}$	$UNQ_{1,3}$	$UNQ_{2,3}$	UNQ_4^{er}
Auto	CRO_0	0,268	0,2691	0,2861	0,2201	0,1985	0,2218	**0,2439**
	CRO_1	0,2705	0,2721	0,2782	0,2468	0,2437	0,2785	**0,265**
	CRO_2	0,3127	**0,3345**	0,2764	0,2966	0,3009	0,2667	**0,298**
	CRO_3	0,2389	0,2413	**0,197**	0,2432	0,2479	0,2377	**0,2343**
Fixed	CRO_0	0,2223	0,1976	0,2323	0,2195	0,2016	0,2401	**0,2189**
	CRO_1	0,2339	0,2504	0,2777	0,2451	0,27	0,2469	**0,254**
	CRO_2	0,2681	0,2658	0,2568	0,2773	0,2779	0,3106	**0,2761**
	CRO_3	0,2531	0,2676	0,2509	0,3081	0,2474	0,2809	**0,268**

Другими словами, уникальность множеств пар симметричных путей, сгенерированных на одном кристалле, эквивалентна уникальности множеств пар, полученных на различных кристаллах. Значения внутрикристальной уникальности лежат в диапазоне [0,1944; 0,3507], а межкристальной уникальности – в диапазоне [0,197; 0,3345], что более чем в 10 раз выше диапазона, представленного ранее [8].

Вычисление характеристики *STA* производилось, как и для предыдущей схемы, при тех же значениях T=10^4 и E=100. Для схемы СККО ФНФ наблюдается уменьшение значений данной характеристики, в связи с наличием большего числа нестабильных пар запрос-ответ. Среднее значение метрики *STA* уменьшилось более чем на 2,5% и составляет для автоматического размещения 0,9694, а для фиксированного – 0,9739.

Связано это с увеличением числа метастабильных пар запрос-ответ, что наглядно можно наблюдать на графиках распределения значений $STA_{CH_i}^E$ по всем копиям схем ФНФ ККО (рис. 5.а), реализованных на ПЛИС $FPGA_3$ в сравнении со схемами ФНФ СККО (рис. 5.б).

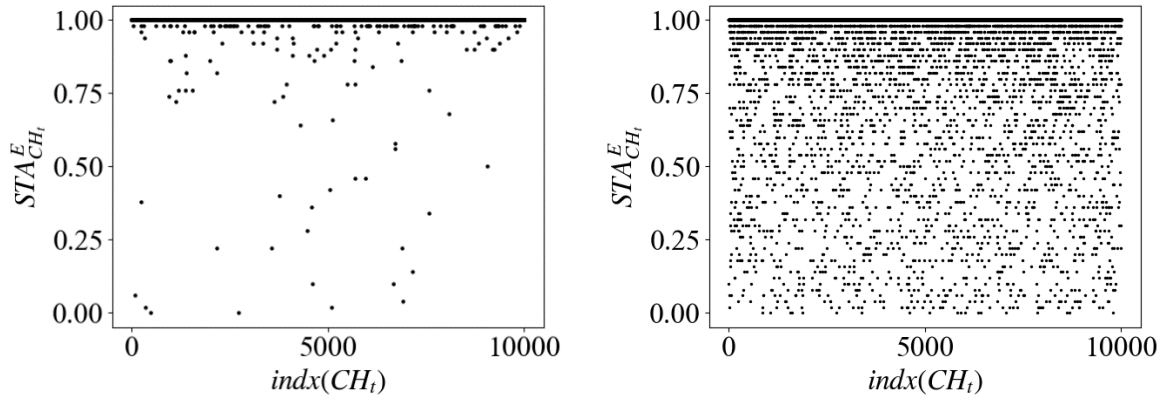

Рис. 5. Значения характеристики $STA^E_{CH_t}$ для всех экземпляров предыдущей схемы ККО (а и для предложенной схемы СККО (б) на $FPGA_3$

В табл. 7 представлены значения числа метастабильных пар запрос-ответ $|CHX|$. для всех исследуемых схем ФНФ ККО и СККО в фиксированном сценарии размещения для параметров T=10^4 и E=100.

В сравнении с предыдущей схемой наблюдается увеличение на порядок числа $|CHX|$. Так, для автоматического размещения среднее число нестабильных пар увеличилось более чем в 24 раза, а для фиксированного – более чем в 11 раз.

Значение характеристики надежности ФНФ *REL* лежит в диапазоне [0,8622; 0,9202], где наименьшее значение относится к схеме CRO_2, реализованной на $FPGA_1$ с автоматическим размещением, а наибольшее значение – к схеме CRO_0, реализованной на той же ПЛИС с фиксированным размещением.

Предложенная новая схема СККО ФНФ за счет реализации множества симметричных конфигурируемых путей на ресурсах LUT-блоков обладает приемлемыми показателями внутрикристальной и межкристальной уникальности в сравнении со схемой ФНФ, для которой симметричные пути реализованы на ресурсах программируемых межсоединений ПЛИС.

Таблица 7. Число метастабильных пар ФНФ ККО и СККО

Размещение	ПЛИС	$\|CHX\|$							
		Схемы ККО				Схемы СККО			
		CRO_0	CRO_1	CRO_2	CRO_3	CRO_0	CRO_1	CRO_2	CRO_3
Auto	$FPGA_0$	86	45	14	33	939	1176	1078	926
	$FPGA_1$	79	28	24	29	1011	976	1211	917
	$FPGA_2$	59	27	29	29	860	985	1064	974
	$FPGA_3$	81	23	28	37	889	1059	1033	832
Fixed	$FPGA_0$	89	40	103	89	818	902	823	771
	$FPGA_1$	77	27	118	32	739	872	961	887
	$FPGA_2$	74	24	139	46	769	762	806	887
	$FPGA_3$	78	42	145	84	769	800	1091	819

Возросшая симметрия путей повлекла за собой увеличение числа метастабильных пар запрос-ответ, что негативно сказалось на таких характеристиках как стабильность и

надежность, минимальные значения которых (0,9694 и 0,8622) все равно можно считать высокими.

В табл. 8 представлены значения основных характеристик исследованных схем ФНФ СККО. Жирным шрифтом отмечены те значения характеристик, которые улучшились в сравнении с ранее рассмотренными схемами (см. табл. 1).

Таблица 8. Значения основных характеристик ФНФ СККО

$\sigma \cdot \mu^{-1}$, %		*REL*		*STA*		*UNF*		UNQ_k^{ra}		UNQ_k^{er}	
min	max	min	max	min	max	min	max	min	max	min	max
0,226	**0,354**	0,8622	0,9202	0,9694	0,9773	0,9756	**1,0**	**0,2333**	**0,2792**	**0,2189**	**0,298**

Приемлемые значения характеристик уникальности возможно достичь путем увеличения длины конфигурируемых симметричных путей, а больших значений стабильности и надежности – при помощи мажоритарного декодирования ответов ФНФ либо с применением помехоустойчивых кодов (коды с повторением, коды Хэмминга, БЧХ-коды) [15, 19]. Кроме этого, использование альтернативных подходов на стадиях измерения задержек распространения сигналов и формирования ответов открывает новые возможности для построения и исследования схем СККО ФНФ различного назначения.

Заключение

Высокая степень асимметрии конфигурируемых путей схем ККО, реализованных на программируемых межсоединениях ПЛИС, негативно сказывается на такой характеристике ФНФ, как межкристальная уникальность. При этом данные схемы обладают достаточно высокими показателями стабильности, надежности и единообразия.

Для увеличения симметрии конфигурируемых путей был предложен подход, основанный на использовании ресурсов технологических блоков LUT, которые обладают высокой степенью внутренней симметрии и идентичностью на различных копиях. Проведенный ряд экспериментов показал состоятельность данного похода, что привело к увеличению показателя межкристальной уникальности более чем в 10 раз с незначительным уменьшением остальных характеристик ФНФ.

СПИСОК ЛИТЕРАТУРЫ:

1. Chang Ch.H., Potkonjak M. Secure System Design and Trustable Computing. Switzerland: Springer, 2016. – 549 p. DOI: https://doi.org/10.1007/978-3-319-14971-4.
2. Hemavathy S. and Bhaaskaran V.S.K. Arbiter PUF–A Review of Design, Composition, and Security Aspects. IEEE Access, v. 11, p. 33979–34004, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3264016.
3. Hajimiri A., Limotyrakis S., Lee T. H. Jitter and phase noise in ring oscillators. IEEE Journal of Solid-state circuits. 2002, v. 34, no. 6, p. 790–804. DOI: https://doi.org/10.1007/0-306-48199-5_5.
4. Deng D., Hou S., Wang Z., Guo Y. Configurable ring oscillator PUF using hybrid logic gates. IEEE Access. 2020, v. 8, p. 161427–161437. DOI: https://doi.org/10.1109/ACCESS.2020.3021205.
5. Deng D. et al. Configurable ring oscillator PUF using hybrid logic gates. IEEE Access. 2020, v. 8, p. 161427–161437. DOI: https://doi.org/10.1109/ACCESS.2020.3021205.
6. Vicuña K. et al. Highly Stable Reconfigurable TERO PUF Architecture for Hardware Security Applications. Transactions on Very Large-Scale Integration (VLSI) Systems. 2025. DOI: https://doi.org/10.1109/TVLSI.2025.3587502.
7. Younes L. et al. DCDC PUF an enhanced implementation of ring oscillator based PUF. Scientific Reports. 2025, v. 15, no. 1, p. 31017. DOI: https://doi.org/10.1038/s41598-025-16221-z.
8. Иванюк А.А. Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора. Информатика. 2025, т. 22, № 1, с. 73–89. DOI: https://doi.org/10.37661/1816-0301-2025-22-1-73-89.
9. Maiti A. et al. A large scale characterization of RO-PUF. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). IEEE, 2010, p. 94–99. DOI: https://doi.org/10.1109/HST.2010.5513108.

10. Martínez-Rodríguez M.C. et al. Efficient RO-PUF for generation of identifiers and keys in resource-constrained embedded systems. Cryptography. 2022, v. 6, no. 4, p. 51. DOI: https://doi.org/10.3390/cryptography6040051.
11. Zhou K. et al. FPGA-based RO PUF with low overhead and high stability. Electronics Letters. 2019, v. 55, no. 9, p. 510–513. DOI: https://doi.org/10.1049/el.2019.0451.
12. Rojas-Muñoz L. F. et al. True random number generation capability of a ring oscillator PUF for reconfigurable devices. Electronics. 2022, v. 11, no. 23, c. 4028. DOI: https://doi.org/10.3390/electronics11234028.
13. Karmakar M., Naz S. F., Shah A. P. Fault-tolerant reversible logic gate-based RO-PUF design. Memories-Materials, Devices, Circuits and Systems. 2023, v. 4, p. 100055. DOI: https://doi.org/10.1016/j.memori.2023.100055.
14. Шамына А.Ю., Иванюк А.А. Построение и балансировка путей физически неклонируемой функции типа арбитр на FPGA. Информатика. 2022;19(4):27–41. DOI: https://doi.org/10.37661/1816-0301-2022-19-4-27-41.
15. Zalivaka, S.S., Zhang, L., Klybik, V.P., Ivaniuk, A.A., Chang, CH. (2016). Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography. In: Chang, CH., Potkonjak, M. (eds) Secure System Design and Trustable Computing. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-14971-4_2.
16. Chiou L.Y., Wu C.H., Wei P. C. A Reliable Delay-Based Physical Unclonable Function with Dark-Bit Avoidance. IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan. 2019, p. 1–4. DOI: https://doi.org/10.1109/ISCAS.2019.8702131.
17. Khan S. et al. A symmetric D flip-flop based PUF with improved uniqueness. Microelectronics Reliability. 2020, v. 106, p. 113595. DOI: https://doi.org/10.1016/j.microrel.2020.113595.
18. Terrence Mak, Crescenzo D'Alessandro, Pete Sedcole, Peter Y. K. Cheung, Alex Yakovlev, and Wayne Luk. 2008. Global interconnections in FPGAs: modeling and performance analysis. In Proceedings of the 2008 international workshop on System level interconnect prediction (SLIP '08). Association for Computing Machinery, New York, NY, USA, 51–58. DOI: https://doi.org/10.1145/1353610.1353621.
19. Yu M.D., Devadas S. Secure and robust error correction for physical unclonable functions. IEEE Design & Test of Computers. 2010, v. 27, no. 1, p. 48–65. DOI: https://doi.org/10.1109/MDT.2010.25.

REFERENCES:

[1] Chang Ch.H., Potkonjak M. Secure System Design and Trustable Computing. Switzerland: Springer, 2016. – 549 p. DOI: https://doi.org/10.1007/978-3-319-14971-4.
[2] Hemavathy S. and Bhaaskaran V.S.K. Arbiter PUF–A Review of Design, Composition, and Security Aspects. IEEE Access, v. 11, p. 33979–34004, 2023. DOI: https://doi.org/10.1109/ACCESS.2023.3264016.
[3] Hajimiri A., Limotyrakis S., Lee T. H. Jitter and phase noise in ring oscillators. IEEE Journal of Solid-state circuits. 2002, v. 34, no. 6, p. 790–804. DOI: https://doi.org/10.1007/0-306-48199-5_5.
[4] Deng D., Hou S., Wang Z., Guo Y. Configurable ring oscillator PUF using hybrid logic gates. IEEE Access. 2020, v. 8, p. 161427–161437. DOI: https://doi.org/10.1109/ACCESS.2020.3021205.
[5] Deng D. et al. Configurable ring oscillator PUF using hybrid logic gates. IEEE Access. 2020, v. 8, p. 161427–161437. DOI: https://doi.org/10.1109/ACCESS.2020.3021205.
[6] Vicuña K. et al. Highly Stable Reconfigurable TERO PUF Architecture for Hardware Security Applications. Transactions on Very Large-Scale Integration (VLSI) Systems. 2025. DOI: https://doi.org/10.1109/TVLSI.2025.3587502.
[7] Younes L. et al. DCDC PUF an enhanced implementation of ring oscillator based PUF. Scientific Reports. 2025, v. 15, no. 1, p. 31017. DOI: https://doi.org/10.1038/s41598-025-16221-z.
[8] Иванюк А.А. Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора. Информатика. 2025, т. 22, № 1, с. 73–89. DOI: https://doi.org/10.37661/1816-0301-2025-22-1-73-89.
[9] Maiti A. et al. A large scale characterization of RO-PUF. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST). IEEE, 2010, p. 94–99. DOI: https://doi.org/10.1109/HST.2010.5513108.
[10] Martínez-Rodríguez M.C. et al. Efficient RO-PUF for generation of identifiers and keys in resource-constrained embedded systems. Cryptography. 2022, v. 6, no. 4, p. 51. DOI: https://doi.org/10.3390/cryptography6040051.
[11] Zhou K. et al. FPGA-based RO PUF with low overhead and high stability. Electronics Letters. 2019, v. 55, no. 9, p. 510–513. DOI: https://doi.org/10.1049/el.2019.0451.
[12] Rojas-Muñoz L. F. et al. True random number generation capability of a ring oscillator PUF for reconfigurable devices. Electronics. 2022, v. 11, no. 23, c. 4028. DOI: https://doi.org/10.3390/electronics11234028.

[13] Karmakar M., Naz S. F., Shah A. P. Fault-tolerant reversible logic gate-based RO-PUF design. Memories-Materials, Devices, Circuits and Systems. 2023, v. 4, p. 100055. DOI: https://doi.org/10.1016/j.memori.2023.100055.
[14] Shamyna A.Yu., Ivaniuk A.A. Creating and balancing the paths of arbiter-based physically unclonable functions on FPGA. Informatics. 2022;19(4):27-41. (In Russ.) DOI: https://doi.org/10.37661/1816-0301-2022-19-4-27-41 (in Russian).
[15] Zalivaka, S.S., Zhang, L., Klybik, V.P., Ivaniuk, A.A., Chang, CH. (2016). Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography. In: Chang, CH., Potkonjak, M. (eds) Secure System Design and Trustable Computing. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-14971-4_2.
[16] Chiou L.Y., Wu C.H., Wei P. C. A Reliable Delay-Based Physical Unclonable Function with Dark-Bit Avoidance. IEEE International Symposium on Circuits and Systems (ISCAS), Sapporo, Japan. 2019, p. 1–4. DOI: https://doi.org/10.1109/ISCAS.2019.8702131.
[17] Khan S. et al. A symmetric D flip-flop based PUF with improved uniqueness. Microelectronics Reliability. 2020, v. 106, p. 113595. DOI: https://doi.org/10.1016/j.microrel.2020.113595.
[18] Terrence Mak, Crescenzo D'Alessandro, Pete Sedcole, Peter Y. K. Cheung, Alex Yakovlev, and Wayne Luk. 2008. Global interconnections in FPGAs: modeling and performance analysis. In Proceedings of the 2008 international workshop on System level interconnect prediction (SLIP '08). Association for Computing Machinery, New York, NY, USA, 51–58. DOI: https://doi.org/10.1145/1353610.1353621.
[19] Yu M.D., Devadas S. Secure and robust error correction for physical unclonable functions. IEEE Design & Test of Computers. 2010, v. 27, no. 1, p. 48–65. DOI: https://doi.org/10.1109/MDT.2010.25.

Статья поступила в редакцию 30.06.2025; одобрена после рецензирования 30.07.2025; принята к публикации 30.08.2025
The article was submitted 30.06.2025; approved after reviewing 30.07.2025; accepted for publication 30.08.2025