ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ СИСТЕМ
INFORMATION PROTECTION AND SYSTEM RELIABILITY

УДК 004.832.32
DOI: 10.37661/1816-0301-2025-22-1-73-89

Оригинальная статья
Original Article

Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора

А. А. Иванюк

Белорусский государственный университет информатики и радиоэлектроники,
ул. П. Бровки, 6, Минск, 220013, Беларусь
E-mail: ivaniuk@bsuir.by

Аннотация

Цели. Целью работы являются рассмотрение особенностей проектирования и реализации физически неклонируемой функции (ФНФ) конфигурируемого кольцевого осциллятора (ККО) на программируемых логических интегральных схемах (ПЛИС) типа FPGA и оценка основных параметров схем ККО и характеристик ФНФ ККО в различных сценариях моделирования и размещения на кристаллах FPGA.

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

Результаты. Предложена обобщенная модель ФНФ, основанная на сравнении задержек распространения сигналов по паре симметричных путей. Модель включает в себя четыре основные стадии: генерирование множества симметричных путей (*Generate*), выборку из множества пары путей (*Select*/*Switch*), измерение задержки распространения сигнала для каждого выбранного пути (*Measure*) и вычисление бинарного ответа ФНФ на основе знака разницы измеренных задержек (*Compute*). Данная модель применима к таким классическим типам ФНФ, как ФНФ типа арбитр и ФНФ кольцевого осциллятора, и к их модификациям. На основе предложенной модели спроектирована ФНФ ККО, которая была реализована на ПЛИС типа FPGA Xilinx ZYNQ 7000. В ходе проведенных экспериментов над моделями и реализованными схемами были оценены основные временные параметры ККО и характеристики ФНФ ККО в различных сценариях моделирования и для двух типов размещения их компонент на кристаллах FPGA. Было показано, что подавляющую часть задержки распространения сигнала по выбранному пути составляет задержка на конфигурируемых межсоединениях FPGA, которая вне зависимости от типа применяемого размещения приводит к реализации множества заведомо асимметричных путей. Нарушение симметрии путей негативно сказывается на одной из важнейших характеристик ФНФ – внутрикристальной уникальности, низкие показатели которой могут служить сильным ограничением при реализации схем неклонируемой идентификации. При этом другие характеристики ФНФ, такие как единообразие, стабильность, надежность и внутрикристальная уникальность, имеют приемлемо высокие показатели.

Заключение. Проведенное параметрическое моделирование схем ФНФ ККО показало свою состоятельность при оценке таких характеристик ФНФ, как единообразие и внутрикристальная уникальность, что может быть использовано разработчиками для быстрой оценки качества проектируемых схем, не прибегая к их реализации. Обеспечение приемлемых значений межкристальной уникальности требует поиска новых схемотехнических решений, которые будут приводить к генерированию множества симметричных путей на ПЛИС типа FPGA. Кроме того, измеренные периоды схем ККО наглядно демон-

стрируют свою уникальность при их реализации как на одном, так и на различных кристаллах, что является основой для поиска новых методов и алгоритмов вычисления уникальных ответов ФНФ.

Ключевые слова: физическая криптография, физически неклонируемые функции, конфигурируемый кольцевой осциллятор, программируемые логические интегральные схемы, симметрия путей

Благодарности. Автор выражает искреннюю благодарность резиденту ПВТ компании «Инженерный Центр Ядро», которая является одним из центров разработки YADRO, за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

Для цитирования. Иванюк, А. А. Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора / А. А. Иванюк // Информатика. – 2025. − Т. 22, № 1. – С. 73–89. – DOI: 10.37661/1816-0301-2025-22-1-73-89.

Конфликт интересов. Автор заявляет об отсутствии конфликта интересов.

Поступила в редакцию | Received 24.01.2025
Подписана в печать | Accepted 07.02.2025
Опубликована | Published 31.03.2025

Investigation of the physically unclonable function of a configurable ring oscillator

Alexander A. Ivaniuk

Belarusian State University
of Informatics and Radioelectronics,
st. P. Brovki, 6, Minsk, 220013, Belarus
E-mail: ivaniuk@bsuir.by

Abstract

Objectives. Design and implementation features of a Physically Unclonable Function (PUF) based on a Configurable Ring Oscillator (CRO) on FPGA platforms are examined. The study aims to evaluate the key parameters of CRO circuits and the characteristics of CRO-based PUFs under various simulation scenarios and placement configurations on FPGA dies.

Methods. Methods of synthesis and analysis of digital devices are employed, including those based on programmable logic integrated circuits, as well as the fundamentals of digital circuit design.

Results. A generalized model of a PUF based on the comparison of signal propagation delays along a pair of symmetric paths is proposed. The model includes four main stages: *Generate* – generating a set of symmetric paths, *Select/Switch* – selecting a pair of paths from the set, *Measure* – measuring the signal propagation delay for each selected path, and *Compute* – calculating the binary PUF response based on the sign of the difference between the measured delays. This model is applicable to classical PUF types such as Arbiter PUFs and Ring Oscillator PUFs, as well as their modifications. Based on the proposed model, a CRO PUF was designed and implemented on Xilinx ZYNQ 7000 FPGA devices. Experiments were conducted on both simulated models and implemented circuits to evaluate the key timing parameters of CROs and the characteristics of CRO PUFs under various simulation scenarios and two types of component placement on FPGA dies. The results demonstrated that the majority of the signal propagation delay along the selected path is determined by the delay in FPGA configurable interconnects. Regardless of the type of component placement used, this leads to the realization of predominantly asymmetric paths. The asymmetry in paths negatively impacts one of the most critical characteristics of PUFs – intra-chip uniqueness. Low intra-chip uniqueness can impose significant limitations when implementing unclonable identification schemes. However, other PUF characteristics, such as uniformity, stability, reliability, and inter-chip uniqueness, exhibited acceptably high-performance levels.

Conclusion. The conducted parametric simulation of CRO PUF circuits demonstrated its effectiveness in evaluating key PUF characteristics, such as uniformity and intra-chip uniqueness. This approach can be utilized by developers for rapid assessment of circuit quality without requiring physical implementation. Achieving acceptable inter-chip uniqueness values necessitates the development of new circuit design solutions that enable the generation of multiple symmetric paths on FPGA devices. Additionally, the measured periods of CRO circuits clearly demonstrate their uniqueness, both when implemented on the same chip and across different chips. This serves as a foundation for exploring new methods and algorithms for calculating unique PUF responses.

Keywords: physical cryptography, physically unclonable functions, configurable ring oscillator, programmable logic integrated circuits, symmetry of paths

Acknowledgments. The author expresses sincere gratitude to the HTP resident company "Engineering Center Yadro", which is one of the YADRO development centers, for providing equipment for conducting experiments as part of the work of a joint educational laboratory with the Belarusian State University of Informatics and Radioelectronics.

For citation. Ivaniuk A. A. *Investigation of the physically unclonable function of a configurable ring oscillator*. Informatika [*Informatics*], 2025, vol. 22, no. 1, pp. 73−89 (In Russ.). DOI: 10.37661/1816-0301-2025-22-1-73-89.

Conflict of interest. The author declares of no conflict of interest.

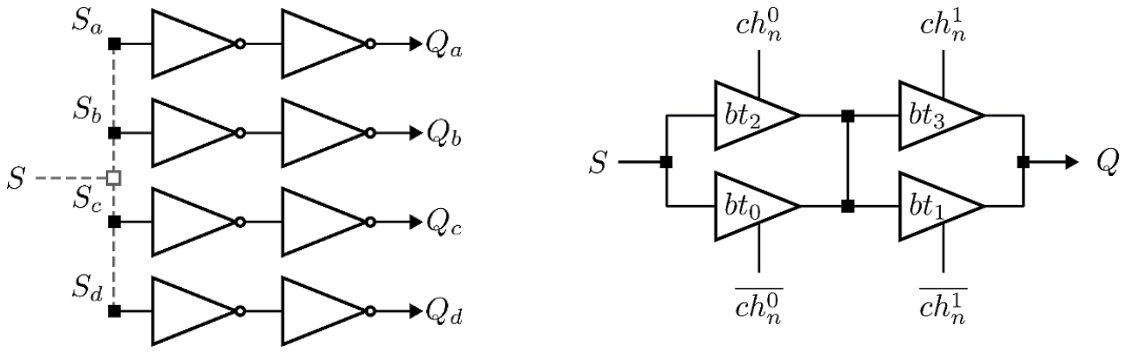
Введение. ФНФ, основанные на извлечении и измерении уникальных физических характеристик полупроводниковых кристаллов цифровых устройств, являются базовыми элементами физической криптографии [1]. К основным областям применения ФНФ можно отнести генерирование случайных чисел и неклонируемую идентификацию, которая, в свою очередь, является основой для методов и средств защиты цифровых устройств от нелегального использования и копирования. Реализованные ФНФ, как правило, представляют собой цифровые схемы, которые достаточно легко проектируются и характеризуются. Однако изготовление схемы ФНФ с заведомо известными характеристиками практически невозможно. Существует достаточное разнообразие схем цифровых ФНФ, большинство из которых основаны на уникальности задержек распространения сигналов. К подобным схемам можно отнести ФНФ типа арбитр [2], ФНФ кольцевых осцилляторов [3], ФНФ конфигурируемых кольцевых осцилляторов [4], ФНФ типа бабочка [5] и др. В настоящей работе делается попытка обобщения подобного класса ФНФ путем создания модели, основанной на множестве симметричных путей, для которых оцениваются значения задержек распространения сигналов. Показано, что наличие симметрии является определяющим фактором работоспособности схем ФНФ. Если симметрия путей может быть достигнута при проектировании и изготовлении заказных СБИС, то для технологий программируемых логических интегральных схем симметрия является практически недостижимой. На базе предложенной модели была спроектирована модифицированная схема ФНФ ККО, основанная на множестве конфигурируемых симметричных путей, с дальнейшей реализацией на программируемых логических интегральных схемах типа FPGA. Приводятся результаты моделирования и анализа основных параметров схем ККО и характеристик ФНФ ККО. Показано, что наличие заведомой асимметрии множества путей негативно сказывается на межкристальной уникальности ФНФ ККО.

ФНФ на основе симметричных путей. Большинство цифровых ФНФ основано на сравнении задержек распространения сигналов по путям, которые проектируются и изготавливаются исходя из предположения, что они являются идентичными. Под путем понимают часть цифровой схемы, для которой определен один вход и один выход. Эта часть схемы состоит из множества цифровых блоков и линий их межсоединений и обеспечивает задержку распространения цифрового сигнала от входа к выходу. Два пути являются симметричными, если множества блоков и межсоединений одного пути совпадают с аналогичными множествами другого пути, что служит необходимым условием равенства их задержек. Можно выделить следующие виды симметрии путей: проектную, топологическую и физическую. *Проектную симметрию* путей можно легко достичь на стадии проектирования цифрового устройства. В свою очередь, проектная симметрия может быть *функциональной* и *схемотехнической* (*структурной*). Так, функциональная симметрия двух путей обеспечивается заданием их эквивалентных поведенческих

проектных описаний, в то время как схемотехническая симметрия – путем задания эквивалентных структурных описаний. *Топологическая симметрия* может быть обеспечена идентичным расположением копий технологических элементов двух путей и геометрическим равенством их соответствующих межсоединений. *Физическая симметрия* может быть в пределе обеспечена при изготовлении полупроводникового кристалла. При этом физическая симметрия бывает двух типов: *внутрикристальная* и *межкристальная*. Если идеальную проектную и топологическую симметрию практически можно обеспечить, то идеальная физическая симметрия недостижима по многим причинам, в первую очередь связанным с девиациями материалов и технологических операций при изготовлении полупроводниковых кристаллов. Это выражается в разности задержек распространения сигналов по симметричным путям, а возможность регистрации такой разности лежит в основе построения цифровых ФНФ.

Для облегчения процесса создания симметричных путей и повышения их идентичности в схемах ФНФ часто применяют конфигурируемые симметричные пути [2, 4], для которых пара сравниваемых путей выбирается посредством задания значения запроса из конечного множества всех возможных запросов $CH \in \{CH_0, CH_1, CH_2, ..., CH_{C-1}\}$.

На рис. 1 приведены примеры симметричных и конфигурируемых симметричных путей, построенных на инверторах и трехстабильных буферах-усилителях. В обеих схемах присутствуют четыре симметричных пути. Для первой схемы (рис. 1, *a*) это пути *a*: (S_a, Q_a), *b*: (S_b, Q_b), *c*: (S_c, Q_c) и *d*: (S_d, Q_d). Во второй схеме каждый из C=4 путей конфигурируется одним из четырех значений $CH_n = (ch_n^0, ch_n^1)$, $n = \overline{0, C-1}$. Так, при $CH_0 = (0,0)$ конфигурируется путь p_0: (S, Q) от входа S до выхода Q через буферные элементы bt_0 и bt_1, а при $CH_3 = (1,1)$ – путь p_3: (S, Q) через элементы bt_2 и bt_3. Оба пути p_0: (S, Q) и p_3: (S, Q) по определению являются симметричными.



a) *b*)

Рис. 1. Схема симметричных путей (*a*) и конфигурируемых симметричных путей (*b*)
Fig. 1. Scheme of symmetrical paths (a) and configurable symmetrical paths (b)

Обе схемы на рис. 1 являются источниками задержек распространения сигналов от входа S до соответствующих выходов. Например, задержка для пути (S_a, Q_a) первой схемы представляет собой суммарную задержку распространения сигнала через два инвертора и транспортную задержку линий межсоединений, связывающих вход S_a с выходом Q_a.

При проектировании представленных схем по технологии заказных СБИС (ASIC) возможно обеспечение проектной и топологической симметрии всех путей. Однако физическая симметрия этих путей после реализации будет нарушена и приобретет уникальный характер в силу многих случайных факторов. С точки зрения обеспечения физической симметрии и экономии аппаратных ресурсов схемы с конфигурируемыми путями являются более предпочтительными. Примерами могут служить схемы ФНФ типа арбитр [2], ФНФ ККО [4] и др.

В общем случае задержку распространения сигнала по физическому пути можно выразить как $\Delta = \Delta_s + \delta_r$, где Δ_s является статической (проектной) составляющей задержки, а $\delta_r \ll \Delta_s$ – динамической случайной составляющей, значение и знак которой определяются внутри- и межкристальными вариациями в изготовленной схеме. При проектировании и параметрическом моделировании цифровых схем значение Δ_s фиксируется для выбранной технологии и условий эксплуатации (design corners) [6]. При этом случайная составляющая δ_r представляется тремя значениями: $\min(\delta_r)$, $\max(\delta_r)$ и $\text{typ}(\delta_r)$, где последнее значение является математическим ожиданием δ_r. Подобное упрощение в представлении задержек нашло применение в стандартном формате описания задержек SDF[1] (Standard Delay Format), широко используемом в современных САПР и средствах статического временного анализа STA[2] (Static Time Analysis).

При проектировании пар симметричных путей можно достичь равенства значений Δ_s, однако после физической реализации случайные значения δ_r приведут к нарушению заложенной на стадии проектирования симметрии.

Результатом сравнения задержек Δ^a и Δ^b двух симметричных путей *a* и *b*, выбранных по некоторому правилу в зависимости от значения запросов, является случайное значение при равенстве их статических составляющих:

$$\Delta^a - \Delta^b = \Delta_s^a - \Delta_s^b + \delta_r^a - \delta_r^b = \delta_r^a - \delta_r^b. \quad (1)$$

Знак приведенной разницы (1) определяет уникальность выбранных симметричных путей и ответ $R \in \{0,1\}$ по следующему правилу:

$$R = \begin{cases} 0, \text{ если } \delta_r^a < \delta_r^b, \\ 1, \text{ если } \delta_r^a \geq \delta_r^b. \end{cases} \quad (2)$$

Если пара путей заведомо является асимметричной, то на различных копиях схемы может наблюдаться одинаковое постоянное значение *R* для выбранного запроса.

Обобщенная модель ФНФ, основанная на сравнении задержек распространения сигналов по паре симметричных путей, изображена на рис. 2.

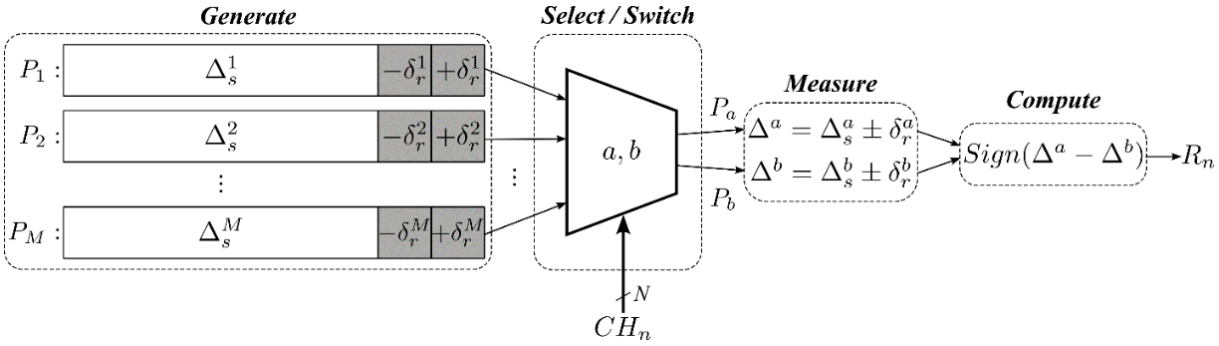


Рис. 2. Обобщенная модель ФНФ
Fig. 2. General PUF model

[1]IEEE Standard for Standard Delay Format (SDF) for the Electronic Design Process : IEEE Std 1497-2001. – 14 Dec. 2001. – 80 p. – DOI: 10.1109/IEEESTD.2001.93359.

[2]Mishagli, D. Statistical Static Timing Analysis of VLSI as the Statistics of Correlated Extremes / D. Mishagli, E. Koskin, E. Blokhina // Arxiv. – URL: https://arxiv.org/html/2401.03559v1 (date of access: 22.01.2025).

Представленная модель содержит четыре основные фазы, последовательность которых приводит к вычислению бита ответа R_n на поданное значение N-разрядного запроса CH_n:

Generate: генерирование множества симметричных путей $P_1, P_2, \ldots, P_M$ при физической реализации цифрового устройства, когда определяются характерные для них уникальные случайные компоненты δ_r^m, $m = \overline{1, M}$;

Select/Switch: при работе готового устройства по значению N-разрядного запроса CH_n ($N \le \lceil \log_2 C_M^2 \rceil$) определенным образом выбирается (*Select*) пара путей с индексами a и b ($a \neq b$), которая далее передается на следующую фазу в прямом $\{P_a, P_b\}$ либо обратном (*Switch*) $\{P_b, P_a\}$ порядке;

Measure: встроенными средствами цифрового устройства осуществляется измерение значений Δ^a и Δ^b для выбранной пары путей;

Compute: согласно равенству (1) осуществляется вычисление бинарного ответа R_n путем установления знака разницы измеренных значений Δ^a и Δ^b.

Общей фазой для всех типов ФНФ является *Generate*. Например, для ФНФ типа арбитр дополнительно выделяют фазы *Select* и *Switch* [7], при этом фаза *Measure* совмещена с фазой *Compute* и выполняется схемой арбитра. Для классической схемы ФНФ кольцевого осциллятора [3] характерны все фазы, представленные на рис. 2.

Характеристики ФНФ. С математической точки зрения ФНФ можно представить как сюръективное отображение $PUF : CH \to R$. В этом изображении каждому уникальному запросу CH_n, являющемуся элементом множества запросов $CH = \{CH_0, CH_1, ..., CH_{2^N-1}\}$, где $CH_n = (ch_n^0, ch_n^1, ..., ch_n^{N-1})$ есть двоичный N-разрядный вектор, $ch_n^i \in \{0,1\}$, $i = \overline{0, N-1}$, $n = \overline{0, 2^N - 1}$, однозначно соответствует бит ответа $R_n \in \{0,1\}$. Таким образом, произвольная ФНФ представляется множеством пар запрос-ответ $< CH, R >= \{(CH_0, R_0), (CH_1, R_1), (CH_2, R_2), ..., (CH_{2^N-1}, R_{2^N-1})\}$.

При многократном извлечении значения ответа R_n для одной и той же пары путей (фиксированного значения запроса CH_n) знак результирующей разницы (1) может изменяться. Связано это со многими факторами, которые могут влиять на значения δ_r^a и δ_r^b, например температурными изменениями кристалла, нестабильностью питающего напряжения, девиацией других неконтролируемых параметров элементов схемы. В таком случае пара запрос-ответ (CH_n, R_n) признается метастабильной. В противном случае, при устойчивом повторении ответа R_n, пара признается стабильной. *Стабильность (stability)* пары на E повторяющихся запросах можно оценить как вероятность появления нулевого либо единичного ответа:

$$STA_{CH_n}^E = 2 \cdot \left| 0,5 - \frac{1}{E} \cdot \sum_{e=0}^{E-1} R_n^e \right|, \tag{3}$$

где R_n^e – ответ, полученный при e-м повторении запроса CH_n.

Тогда стабильность всей ФНФ можно оценить следующей формулой:

$$STA = \frac{1}{2^N} \cdot \sum_{n=0}^{2^N-1} STA_{CH_n}^E . \tag{4}$$

Пусть $< CH, 0 >^E$ есть множество пар запрос-ответ со стабильным нулевым ответом, для которых $STA_{CH_n}^E = 1$. Тогда $< CH, 1 >^E$ – множество пар со стабильным единичным ответом,

а $< CH, X >^E$ – множество пар с метастабильным ответом, $STA^E_{CH_n} < 1$. Очевидно, что $< CH, R >^E = < CH, 0 >^E \cup < CH, 1 >^E \cup < CH, X >^E$, $|< CH, R >^E| = 2^N$.

Соотношение множеств стабильных и метастабильных пар определяет одну из важнейших характеристик ФНФ – *надежность (reliability)*:

$$REL = 1 - \frac{\left| < CR, X >^E \right|}{\left| < CR, 0 >^E \right| + \left| < CR, 1 >^E \right|}. \quad (5)$$

Множество стабильных пар может быть применено для решения задачи уникальной идентификации цифрового устройства, в то время как множество метастабильных пар – для генерирования случайных данных. В задачах уникальной идентификации метастабильные пары нивелируются, например, путем их стабилизации при помощи механизмов помехоустойчивого декодирования либо путем исключения их из рассмотрения. Последующие характеристики ФНФ основаны на утверждении, что $< CH, R >^E = < CH, 0 >^E \cup < CH, 1 >^E$.

Другой важной характеристикой ФНФ является *случайность*, определяемая соотношением мощностей множеств пар $< CH, 0 >$ и $< CH, 1 >$ и выражаемая нормированной метрикой *единообразия (uniformity)*:

$$UNI = 1 - 2 \cdot \left| 0,5 - \frac{|< CH, 1 >|}{|< CH, R >|} \right|. \quad (6)$$

Если мощность множества $|< CH, R >|$ достаточно велика, например N=64 и более, то для получения вышеописанных и других характеристик используют меньшее число запросов $T \ll 2^N$, равномерно распределенных по множеству всех возможных запросов и генерируемых, как правило, псевдослучайным образом.

Так, для сравнения двух копий i и j ФНФ применяют метрику *уникальности (uniqueness)*:

$$UNQ_{i,j} = 1 - \frac{1}{T} \cdot \left| < CH, R >_i \bigcap < CH, R >_j \right|, \quad (7)$$

по сути, представляющую собой удельное расстояние по Хэммингу между двумя векторами ответов двух ФНФ, полученных при подаче T различных запросов.

При сравнении k >2 копий ФНФ можно применять формулу

$$UNQ_k = \frac{1}{C_k^2} \cdot \sum_{i=1}^{k-1} \sum_{j=2}^{k} UNQ_{i,j}, \quad (8)$$

определяющую математическое ожидание уникальности всех возможных пар сравниваемых копий.

Метрика UNQ_k, рассчитанная для копий ФНФ, реализованных на одном кристалле, определяет *внутрикристальную уникальность* (*Intra* UNQ_k), а для копий ФНФ, реализованных на идентичных кристаллах, – *межкристальную уникальность* (*Inter* UNQ_k).

При реализации уникальной идентификации одной из важных задач исследователей и проектировщиков схем ФНФ является достижение значений перечисленных характеристик (4)–(7) близкими к значению 1, а характеристики (8) – к значению 0,5. В то же время при проектировании схем генераторов случайных чисел стремятся достичь значений *STA* и *REL*, близких к 0.

Обеспечение симметрии путей является определяющей задачей при построении схем ФНФ с высокими значениями их характеристик. В противном случае, если пары исследуемых путей не являются симметричными, то это в первую очередь негативно сказывается на такой характеристике, как уникальность. Как уже было отмечено, для ASIC-технологий возможно обеспечение симметрии конфигурируемых путей, однако для ПЛИС подобная реализация затруднена. С одной стороны, ПЛИС, например, типа FPGA, по сути, является полупроводниковым кристаллом, выполненным по технологии ASIC, но пути в ней реализуются посредством конфигурируемых связей, имеющих заведомую физическую асимметрию [8]. Кроме того, задержки распространения сигналов по конфигурируемым межсоединениям в FPGA заметно превосходят задержки на функциональных элементах, реализуемых, например, на LUT-блоках [9]. Рассмотрим эти особенности на примере реализации ФНФ типа ККО на FPGA и оценим приведенные основные характеристики данного вида ФНФ.

ФНФ типа ККО. Общая схема ККО (англ. CRO, Configurable Ring Oscillator) может быть представлена в качестве схемы задержки и управляемого инвертора, реализованного, как правило, при помощи вентиля NAND2, которые объединены петлей обратной связи [10]. Схема задержки при этом представляет собой M конфигурируемых симметричных путей (фаза *Generate*). Для построения схемы ФНФ на основе ККО необходимо наличие синхронных счетчиков CNT_1 и CNT_2 (фаза *Measure*), схемы компаратора *CMP* (фаза *Compute*) и устройства управления *CONTROL*, вырабатывающего необходимые последовательности сигналов. Кроме этого, *CONTROL* осуществляет выработку значений двух конфигураций CH_a и CH_b для ККО на основе подаваемого значения запроса CH_n (фаза *Select/Switch*) (рис. 3).

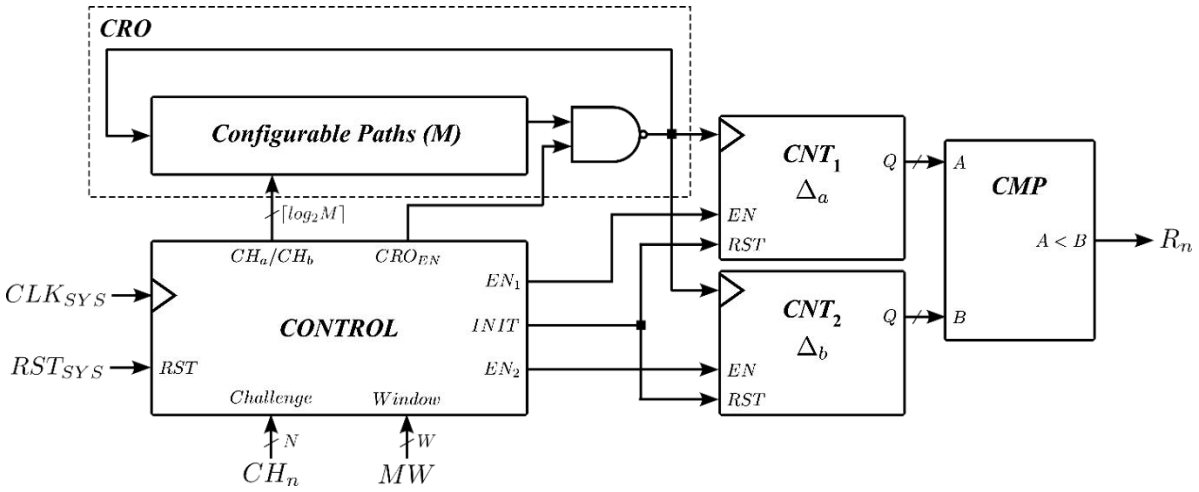


Рис. 3. Обобщенная модель ФНФ типа ККО

Fig. 3. Generalized model of CRO PUF

Изначально значения счетчиков обнуляются путем подачи сигнала *INIT* от блока управления. Затем на основе поданного запроса CH_n вырабатываются два значения конфигурации CH_a и CH_b, которые последовательно подаются на схему ККО. Выбранный путь по первичному значению CH_a из множества M симметричных путей формирует уникальную задержку в цепи обратной связи схемы ККО, которая оценивается на счетчике CNT_1 путем подсчета полных периодов генерируемого сигнала во временном окне измерения, задаваемого входным значением *MW* блока управления. Описанная последовательность действий повторяется для конфигурации CH_b с подсчетом полных периодов сигнала на счетчике CNT_2. В итоге значения двух счетчиков сравниваются на компараторе с выработкой бинарного ответа R_n. Рассмотренная схема может быть упрощена в части применения одного счетчика с прямым счетом для конфигурации CH_a и обратным для конфигурации CH_b в дополнительном коде [11]. Тогда итоговый знак значения счета и будет определять ответ схемы R_n.

Рассмотрим практическую схему ФНФ ККО, реализованную на ПЛИС типа FPGA Xilinx ZYNQ 7000, которая имеет следующие параметры: M=1024 и N=19. Схема конфигурируемых симметричных путей построена на пяти мультиплексорах MUX4x1. Все мультиплексоры последовательно соединены между собой и управляются 10-разрядной шиной конфигурации CF. Выбор такой схемы был обусловлен компактным размещением схем MUX4x1 на технологических элементах LUT6 кристалла FPGA. На рис. 4 показан результат технологического синтеза исследуемой схемы, включающий в себя пять блоков LUT6 ($L0$ – $L4$) и блок LUT2 ($A0$), который реализует управляемый инвертор схемы ККО.

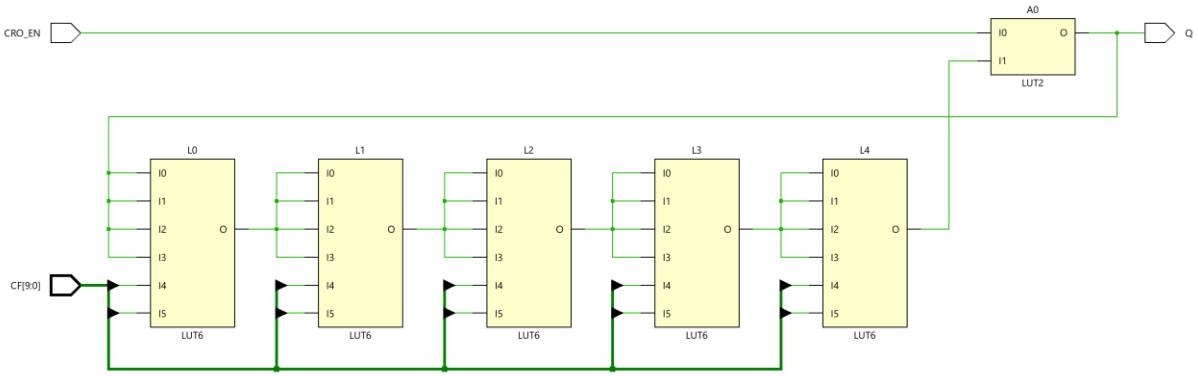
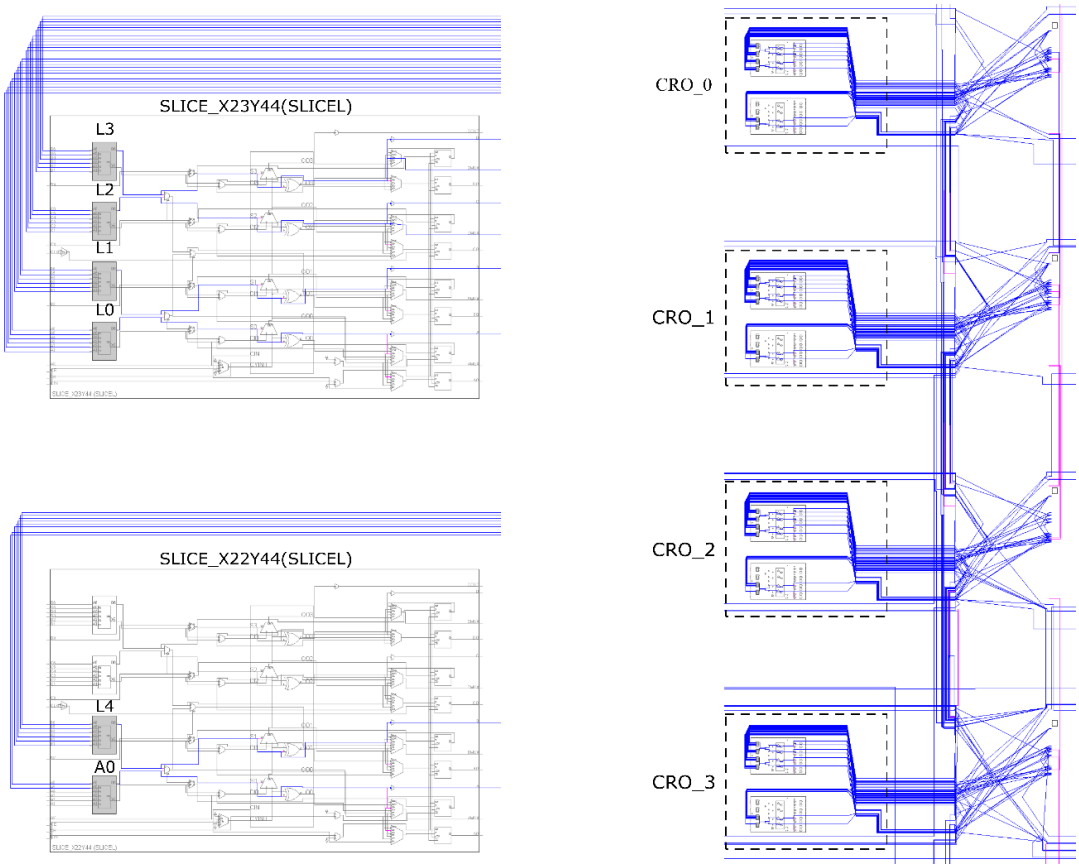


Рис. 4. Схема исследуемого ККО

Fig. 4. Scheme of studied CRO



a) *b)*

Рис. 5. Фиксированное размещение компонент одной схемы ККО (*a*) и четырех схем ККО (*b*) на ресурсах FPGA

Fig. 5. Fixed placement of components of one CRO circuit (a) and four CRO circuits (b) on FPGA resources

Для оценки основных характеристик ФНФ ККО в проекте были спроектированы четыре идентичные схемы (CRO_0 – CRO_3), впоследствии реализованные на четырех идентичных кристаллах ПЛИС ($FPGA_0$ – $FPGA_3$). Непосредственно перед реализацией были предварительно оценены симметричные пути посредством измерения периодов генерируемых сигналов при помощи параметрических моделей схем в различных сценариях моделирования, полученных после технологического синтеза. Кроме того, оценка симметрии производилась в двух вариантах размещения схем ККО: варианте автоматического размещения LUT-блоков и трассировки их межсоединений (Auto) и варианте фиксированного размещения (Fixed), при котором на этапе задания проектного описания указывалось конкретное размещение LUT-блоков, а межсоединения закреплялись путем описания их подключений к конкретным физическим входам. После этого фиксированное размещение одной схемы дублировалось на смежных ресурсах идентичных SLICE-блоков для обеспечения максимального подобия четырех компонент ФНФ ККО (рис. 5).

Результаты экспериментальных исследований. До реализации схем оценим симметрию их путей при помощи параметрических моделей, полученных на стадии технологического синтеза.

В САПР Vivado и симуляторе QuestaSim есть возможность оценить два типа задержек распространения сигналов: минимальную (Min) и максимальную (Max) – для двух условий эксплуатации (design corners): Fast и Slow. С учетом двух видов размещения (Auto и Fixed) можно получить восемь оценок задержек распространения сигналов для технологических моделей схем до их реализации. Например, задержка для блока LUT6 при условии Fixed/Fast/Min составляет 45 пс, при Fixed/Fast/Max – 56 пс, при Fixed/Slow/Min – 100 пс, а при Fixed/Slow/Max – 124 пс. Аналогичные оценки можно получить для межсоединений схемы. Например, значения задержек на линиях, соединяющих выход O блока L3 со входами I0, I1, I2 и I3 блока L4 (см. рис. 4), при условии Fixed/Fast/Min составляют: для линии L3/O:L4/I0 – 390,7 пс; для линии L3/O:L4/I1 – 340,4 пс; для линии L3/O:L4/I2 – 226 пс, а для линии L3/O:L4/I3 – 314,3 пс соответственно. На этом примере видно, что значения задержек на линиях межсоединений многократно превышают задержки на LUT-блоках и являются неравными. Это приводит к реализации заведомо асимметричных путей. Оценку периодов τ сигналов, генерируемых всеми четырьмя компонентами ККО на всех возможных 2^{10} конфигурациях, произведем на восьми моделях и двух вариантах их реализации (Auto и Fixed) на ПЛИС.

На рис. 6 и 7 приведены значения плотностей вероятностей моделируемых и реальных периодов, а в табл. 1 – основные статистические и вероятностные характеристики периодов для всех моделей и реальных схем ККО, реализованных на четырех ПЛИС типа FPGA. На рис. 6 видно, что реальные периоды сигналов схем ККО лежат ближе к модельным оценкам Fast/Max вне зависимости от типа размещения. Больший разброс (разнообразие) значений периодов наблюдается при модельных оценках автоматического размещения компонент ККО, для которых также характерны меньшие значения самих периодов, обусловленные более короткими межсоединениями структурных элементов в сравнении с их фиксированным размещением.

Схожие оценки получены и на реальных схемах (рис. 7, *a* и *b*), для которых также были оценены распределения периодов каждой схемы ККО при реализации на других ПЛИС. При этом наблюдается схожесть относительного распределения периодов на различных кристаллах вне зависимости от типа использованного размещения (рис. 7, *c* и *d*).

Если фиксированное размещение позволило сделать более схожими компоненты ККО, то различие в симметричных путях все равно осталось существенным. Так, для реальных схем диапазоны изменения периодов в автоматическом и фиксированном размещении составляют 3,295 и 3,803 нс соответственно (табл. 2).

Рассмотрим, как влияют приведенные данные на основные характеристики схем ФНФ ККО. Так, до реализации на ПЛИС на полученных параметрических моделях есть возможность оценить такие характеристики, как единообразие (6) и внутрикристальная уникальность (7). Для этого были созданы программные модели ФНФ на базе синтезированных схем ККО,

для которых получены $T=10^4$ ответов на псевдослучайно сгенерированные запросы. Аналогичные запросы были поданы и на реальные схемы ККО, в том числе для оценки других характеристик.

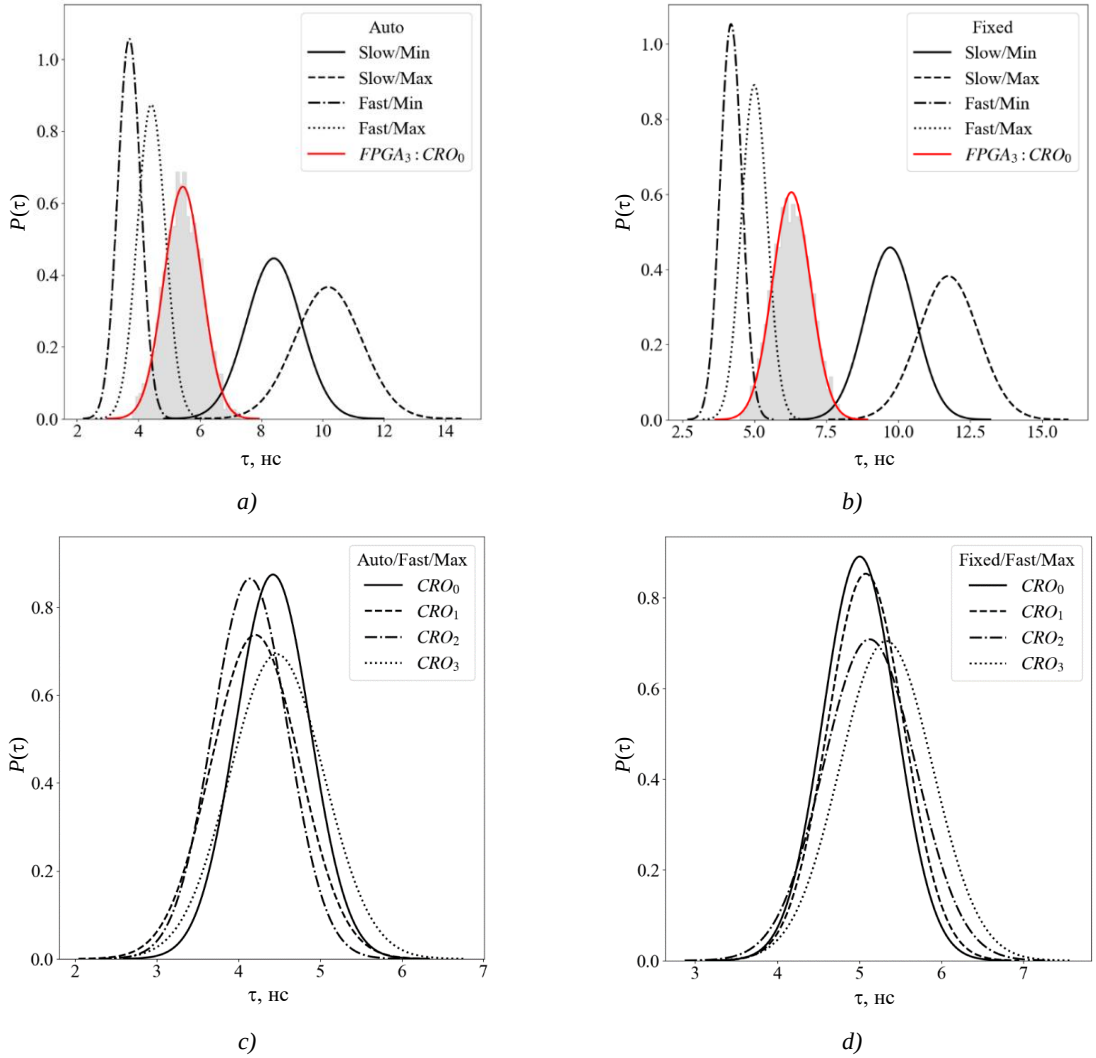


Рис. 6. Плотность вероятности $P(\tau)$ периодов τ компоненты CRO_0 в различных сценариях моделирования и типах размещения в сравнении с реальной компонентой на $FPGA_3$ (*a*, *b*) и для моделей всех компонент в сценарии Fast/Max (*c*, *d*)

Fig. 6. Probability density $P(\tau)$ of periods τ of component CRO_0 in various modeling scenarios and placement types compare to a real component on $FPGA_3$ (a, b) and for models of all components in the Fast/Max scenario (c, d)

В табл. 3 приведены результаты полученных характеристик *UNI*, а в табл. 4 – характеристик внутрикристальной уникальности UNQ_{ij} и UNQ_4 для всех моделей и схем ФНФ ККО. Из представленных данных видно, что все модели и схемы ФНФ ККО обладают достаточно высокими значениями метрики единообразия вне зависимости от типа размещения компонент на кристалле FPGA и в различных сценариях моделирования. Обусловлено это в первую очередь подавляющим большинством реализованных путей различной протяженности в схемах ККО, что асимптотически позволяет генерировать равные по мощности множества единичных и нулевых ответов (см. рис. 2).

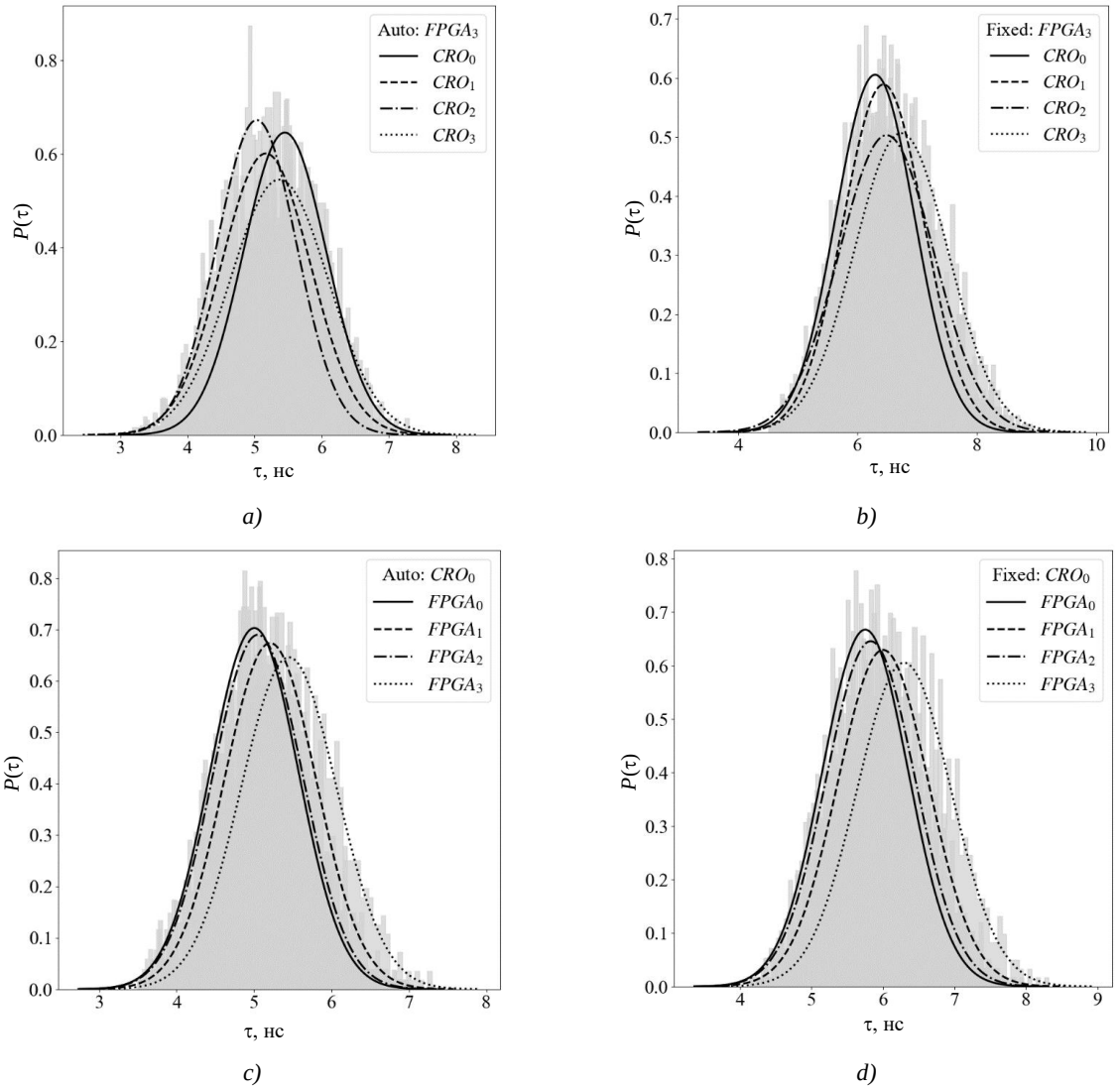


Рис. 7. Плотность вероятности $P(\tau)$ периодов τ всех компонент в различных типах размещения на кристалле $FPGA_3$ (*a, b*) и для компоненты CRO_0, реализованной на различных ПЛИС (*c, d*)

Fig. 7. Probability density $P(\tau)$ of periods τ of all components in various placement types on the $FPGA_3$ (a, b) and for the CRO_0 component implemented on various FPGAs (c, d)

В свою очередь, метрика внутрикристальной уникальности схем ФНФ ККО существенно снижается при фиксированном варианте размещения компонент в сравнении с их автоматическим размещением (см. табл. 4). Это может быть объяснено большой схожестью технологических схем ККО, которые после синтеза располагаются на идентичных ресурсах ПЛИС (см. рис. 5). Подобное поведение значений *Intra INQ* наблюдается как для моделей, так и для реальных схем ККО.

Еще меньшее различие между схемами ФНФ ККО наблюдается при реализации их копий на идентичных ПЛИС, о чем свидетельствуют крайне малые значения метрики *Inter UNQ* (см. табл. 5), которые практически не зависят от типа использованного размещения компонент схем.

Что касается метрики стабильности *STA*, то ее значения, так же как и значения единообразия для всех исследуемых схем ККО, реализованных на различных ПЛИС, являются весьма высокими (две-три девятки после запятой). Например, для схемы CRO_0, реализованной на $FPGA_0$ при автоматическом размещении, было получено значение *STA*=0,99905, а для этой же схемы

в фиксированном размещении – значение *STA*=0,99926. Вычисление данной метрики проходило при параметрах $T=10^4$ и $E=100$.

Таблица 1
Характеристики периодов сигналов моделей ККО в различных сценариях моделирования и типах размещения
Table 1
Characteristics of signal periods of CRO models in various simulation scenarios and placement types

Сценарий *Scenario*		ККО *CRO*	min(*T*), нс min(*T*), *ns*		max(*T*), нс max(*T*), *ns*		Математическое ожидание μ, нс *Expected value* μ, *ns*		СКО σ, нс *Standard deviation* σ, *ns*		σ/μ, %	
			Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed
Slow	Max	CRO_0	7,212	8,876	13,436	14,918	10,185	11,748	1,088	1,043	10,685	8,882
		CRO_1	6,410	8,846	12,698	15,098	9,789	11,885	1,260	1,082	12,869	9,103
		CRO_2	6,480	8,846	12,434	15,902	9,701	12,028	1,102	1,255	11,354	10,433
		CRO_3	6,414	8,872	13,394	15,902	10,292	12,354	1,277	1,273	12,410	10,305
	Min	CRO_0	5,964	7,340	11,090	12,362	8,416	9,723	0,894	0,870	10,621	8,949
		CRO_1	5,138	7,310	10,232	12,514	7,972	9,845	1,033	0,904	12,952	9,185
		CRO_2	5,380	7,310	10,266	13,192	8,030	9,955	0,905	1,052	11,267	10,566
		CRO_3	5,310	7,336	11,056	13,186	8,524	10,235	1,058	1,063	12,412	10,388
Fast	Max	CRO_0	3,178	3,782	5,778	6,392	4,423	5,005	0,456	0,448	10,318	8,949
		CRO_1	2,764	3,752	5,458	6,448	4,207	5,077	0,541	0,468	12,870	9,212
		CRO_2	2,828	3,752	5,320	6,860	4,143	5,125	0,461	0,563	11,132	10,991
		CRO_3	2,750	3,778	5,842	6,874	4,471	5,327	0,576	0,566	12,876	10,632
	Min	CRO_0	2,662	3,168	4,824	5,362	3,702	4,195	0,377	0,379	10,191	9,030
		CRO_1	2,268	3,138	4,504	5,406	3,497	4,257	0,453	0,396	12,946	9,312
		CRO_2	2,388	3,138	4,446	5,764	3,478	4,293	0,382	0,481	10,986	11,198
		CRO_3	2,310	3,164	4,882	5,776	3,755	4,472	0,485	0,481	12,918	10,751

Таблица 2
Характеристики периодов сигналов реальных ККО в различных типах размещения
на различных ПЛИС
Table 2
Characteristics of signal periods of real CROs in various types of placement on different FPGAs

ПЛИС *FPGA*	ККО *CRO*	min(*T*), нс min(*T*), *ns*		max(*T*), нс max(*T*), *ns*		Математическое ожидание μ, нс *Expected value* μ, *ns*		СКО σ, нс *Standard deviation* σ, *ns*		σ/μ, %	
		Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed
$FPGA_0$	CRO_0	3,489	4,133	6,713	7,590	5,003	5,752	0,567	0,598	11,343	10,392
	CRO_1	3,124	4,111	6,092	7,641	4,718	5,834	0,603	0,612	12,773	10,485
	CRO_2	3,062	4,136	5,988	8,105	4,594	5,911	0,539	0,718	11,734	12,142
	CRO_3	2,922	4,137	6,544	8,055	4,939	6,094	0,671	0,705	13,590	11,564
$FPGA_1$	CRO_0	3,627	4,296	6,989	7,968	5,209	6,001	0,592	0,634	11,368	10,561
	CRO_1	3,254	4,307	6,348	8,038	4,932	6,138	0,631	0,650	12,798	10,594
	CRO_2	3,187	4,334	6,217	8,548	4,796	6,205	0,560	0,762	11,671	12,276
	CRO_3	3,060	4,344	6,802	8,468	5,149	6,404	0,702	0,742	13,625	11,584
$FPGA_2$	CRO_0	3,506	4,157	6,779	7,732	5,048	5,827	0,578	0,618	11,457	10,602
	CRO_1	3,151	4,161	6,170	7,810	4,780	5,964	0,616	0,633	12,885	10,607
	CRO_2	3,070	4,171	6,011	8,203	4,632	5,973	0,542	0,734	11,693	12,292
	CRO_3	2,985	4,202	6,605	8,192	5,006	6,196	0,675	0,720	13,491	11,622
$FPGA_3$	CRO_0	3,796	4,504	7,295	8,316	5,450	6,294	0,618	0,659	11,333	10,467
	CRO_1	3,407	4,522	6,681	8,379	5,168	6,435	0,664	0,677	12,840	10,524
	CRO_2	3,294	4,514	6,513	8,893	5,031	6,486	0,593	0,793	11,790	12,225
	CRO_3	3,180	4,547	7,093	8,925	5,367	6,731	0,731	0,788	13,628	11,700

Таблица 3
Значения метрики единообразия *UNI* схем ФНФ ККО в различных сценариях моделирования и размещения

Table 3
Values of the UNI uniformity metric of CRO PUF schemes in various modeling and placement scenarios

Сценарий/ ПЛИС *Scenario/ FPGA*	CRO_0		CRO_1		CRO_2		CRO_3	
	Auto	Fixed	Auto	Fixed	Auto	Fixed	Auto	Fixed
Slow/Min	0,9914	0,9894	0,993	0,9972	0,9934	0,992	0,9992	0,9894
Slow/Max	0,9956	0,9898	0,9932	0,9952	0,9914	0,9914	0,9984	0,99
Fast/Min	0,993	0,988	0,9976	0,9968	0,993	0,9932	0,997	0,993
Fast/Max	0,9958	0,99	0,9932	0,9968	0,9928	0,994	0,9972	0,9928
$FPGA_0$	0,9928	0,994	0,9908	0,9996	0,9914	0,994	0,9998	0,9966
$FPGA_1$	0,9928	0,9912	0,9908	0,9968	0,99	0,9912	0,9996	0,9966
$FPGA_2$	0,993	0,9942	0,9918	0,9984	0,993	0,9936	0,9992	0,9988
$FPGA_3$	0,9938	0,9914	0,9916	0,9966	0,9888	0,9952	0,9994	0,9982

Таблица 4
Значения метрики внутрикристальной уникальности схем ФНФ ККО

Table 4
Values of the metric of intra-chip uniqueness of CRO PUF circuits

Сценарий/ ПЛИС *Scenario/ FPGA*			Внутрикристальная уникальность *Intra UNQ* *Intra-chip uniqueness Intra UNQ*						
			$UNQ_{0,1}$	$UNQ_{0,2}$	$UNQ_{0,3}$	$UNQ_{1,2}$	$UNQ_{1,3}$	$UNQ_{2,3}$	UNQ_4
Auto	Slow	Min	0,4966	0,2578	0,4893	0,4194	0,3091	0,3823	0,3924
		Max	0,4836	0,2539	0,4842	0,3949	0,313	0,3783	0,3846
	Fast	Min	0,5061	0,2568	0,4942	0,4107	0,3327	0,394	0,3991
		Max	0,4899	0,2547	0,4869	0,389	0,33	0,3854	0,3893
Fixed	Slow	Min	0,1447	0,0779	0,1106	0,1928	0,0949	0,1545	0,1292
		Max	0,1413	0,0764	0,1099	0,1889	0,093	0,1517	0,1269
	Fast	Min	0,1412	0,0956	0,1171	0,1926	0,0857	0,1719	0,134
		Max	0,1386	0,0934	0,1176	0,189	0,084	0,1676	0,1317
Auto	$FPGA_0$		0,4798	0,4798	0,4719	0,3947	0,3381	0,3856	0,3882
	$FPGA_1$		0,4854	0,4854	0,472	0,4062	0,3422	0,3858	0,3918
	$FPGA_2$		0,4832	0,4832	0,4715	0,403	0,3423	0,3839	0,3909
	$FPGA_3$		0,4843	0,4843	0,475	0,4038	0,3421	0,3853	0,3922
Fixed	$FPGA_0$		0,1214	0,1214	0,0965	0,161	0,0697	0,1463	0,1124
	$FPGA_1$		0,1274	0,1274	0,1001	0,1658	0,0753	0,1463	0,1145
	$FPGA_2$		0,1255	0,1255	0,1005	0,1712	0,0732	0,148	0,1161
	$FPGA_3$		0,1214	0,1214	0,0968	0,1665	0,0716	0,1501	0,1144

На рис. 8 изображены графики распределения значений $STA^E_{CH_n}$ по всем копиям схем ФНФ ККО, реализованных на ПЛИС $FPGA_3$ для двух вариантов размещения (по осям абсцисс приведены условные индексы использованных псевдослучайных запросов). Видно, что большее число нестабильных пар запрос-ответ наблюдается для фиксированного размещения в сравнении с автоматическим размещением. Это, в свою очередь, сказывается на значениях метрик стабильности *STA* и надежности *REL*. Так, среднее значение метрики *STA* для всех схем при автоматическом размещении составляет 0,9993, а при фиксированном – 0,9989.

Таблица 5
Значения метрик межкристальной уникальности схем ФНФ ККО

Table 5
Values of the metric of inter-chip uniqueness of CRO PUF circuits

Размещение *Placement*	ККО *CRO*	Межкристальная уникальность *Inter UNQ* *Inter-chip uniqueness Inter UNQ*						
		$UNQ_{0,1}$	$UNQ_{0,2}$	$UNQ_{0,3}$	$UNQ_{1,2}$	$UNQ_{1,3}$	$UNQ_{2,3}$	UNQ_4
Auto	CRO_0	0,01	0,0109	0,0119	0,0103	0,0111	0,0096	0,0106
	CRO_1	0,0086	0,0051	0,0072	0,0079	0,0086	0,0067	0,0074
	CRO_2	0,0113	0,0094	0,0145	0,0079	0,0084	0,0099	0,0102
	CRO_3	0,0067	0,0055	0,0076	0,005	0,0055	0,0061	0,0061
Fixed	CRO_0	0,011	0,0089	0,0101	0,0093	0,0075	0,0106	0,0096
	CRO_1	0,0112	0,0154	0,0207	0,0098	0,0137	0,0161	0,0145
	CRO_2	0,0102	0,0108	0,0088	0,0104	0,0122	0,011	0,0106
	CRO_3	0,008	0,0101	0,0068	0,0105	0,0084	0,0067	0,0084

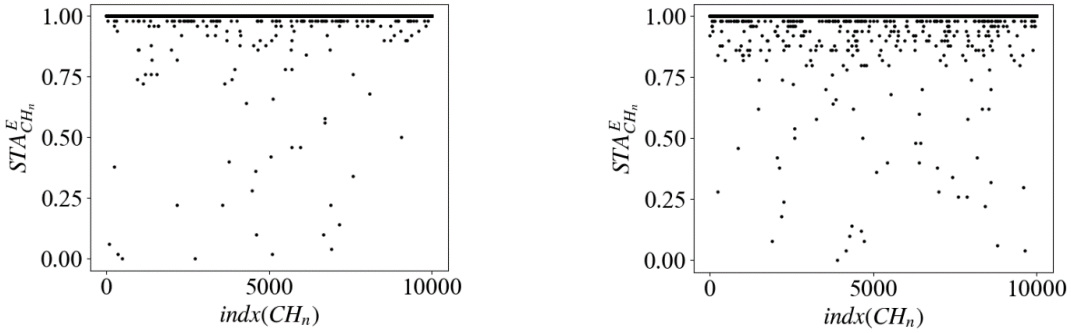


Рис. 8. Значения метрики $STA^E_{CH_n}$ для всех схем ФНФ ККО, реализованных в автоматическом (*a*) и фиксированном (*b*) расположении на $FPGA_3$

Fig. 8. $STA^E_{CH_n}$ metric values for all CRO PUF schemes implemented in automatic (a) and fixed (b) placement of $FPGA_3$

В табл. 6 представлены значения числа метастабильных пар запрос-ответ $|< CR, X >^E|$ (5) для всех исследуемых схем ФНФ ККО в двух сценариях размещения. Как видно из представленных данных, суммарное число метастабильных пар ФНФ при фиксированной реализации почти в 1,85 раза больше, чем при автоматическом размещении, что свидетельствует о большей схожести сравниваемых пар путей схем ККО.

Таблица 6
Число метастабильных пар ФНФ ККО

Table 6
The number of metastable pairs of CRO PUF

Размещение *Placement*	ПЛИС *FPGA*	$\|< CR, X >^E\|$			
		CRO_0	CRO_1	CRO_2	CRO_3
Auto	$FPGA_0$	86	45	14	33
	$FPGA_1$	79	28	24	29
	$FPGA_2$	59	27	29	29
	$FPGA_3$	81	23	28	37
Fixed	$FPGA_0$	89	40	103	89
	$FPGA_1$	77	27	118	32
	$FPGA_2$	74	24	139	46
	$FPGA_3$	78	42	145	84

Значение метрики надежности ФНФ *REL* лежит в диапазоне [0,9853; 0,9986], где наименьшее значение относится к схеме CRO_2, реализованной на $FPGA_3$ с фиксированным размещением, а наибольшее значение – к той же схеме, реализованной на $FPGA_0$ с автоматическим размещением.

Таким образом, можно констатировать, что реализованные на ПЛИС схемы ФНФ ККО обладают приемлемыми показателями единообразия, внутрикристальной уникальности, стабильности и надежности при автоматическом размещении их компонент.

Фиксированное размещение увеличивает степень схожести сравниваемых путей схем ККО, о чем свидетельствует уменьшение показателей внутрикристальной уникальности, стабильности и надежности. Однако вне зависимости от типа используемого размещения все схемы ФНФ ККО обладают неприемлемыми показателями межкристальной уникальности, что может являться сильным ограничением на их практическое применение для схем уникальной идентификации.

Заключение. В статье рассмотрены общие принципы проектирования ФНФ на основе конфигурируемых симметричных путей. Выделены четыре основные фазы функционирования подобных схем: *Generate, Select/Switch, Measure* и *Compute*. На примере схем ККО показано, что фаза *Generate* является определяющей для основных характеристик ФНФ при их реализации на ПЛИС. Высокая степень асимметрии конфигурируемых путей ККО, реализованных на программируемых межсоединениях, негативно сказывается на такой характеристике, как межкристальная уникальность. Было показано также, что некоторые характеристики ФНФ (единообразие и внутрикристальная уникальность) могут быть предварительно оценены на параметрических моделях после синтеза в зависимости от различных типов размещения компонент на кристалле. Проведенные эксперименты с различными схемами ФНФ ККО показали адекватность модельных оценок в сравнении с оценками, полученными на реальных ПЛИС.

Дальнейшие исследования могут быть направлены на поиск новых схемотехнических и аналитических методов улучшения характеристик уникальности для ФНФ, основанных на анализе задержек распространения сигналов по симметричным путям.

Список использованных источников

1. Secure System Design and Trustable Computing / ed.: Ch. H. Chang, M. Potkonjak. – Switzerland : Springer, 2016. – 549 p. – DOI: 10.1007/978-3-319-14971-4.

2. Hemavathy, S. Arbiter PUF – a review of design, composition, and security aspects / S. Hemavathy, V. S. K. Bhaaskaran // IEEE Access. – 2023. – Vol. 11. – P. 33979–34004. – DOI: 10.1109/ACCESS.2023.3264016.

3. Maiti, A. Improved ring oscillator PUF: An FPGA-friendly secure primitive / A. Maiti, P. Schaumont // Journal of Cryptology. – 2011. – Vol. 24. – P. 375–397. – DOI: 10.1007/s00145-010-9088-4.

4. Configurable ring oscillator PUF using hybrid logic gates / D. Deng, S. Hou, Z. Wang, Y. Guo // IEEE Access. – 2020. – Vol. 8. – P. 161427–161437. – DOI: 10.1109/ACCESS.2020.3021205.

5. Extended abstract: The butterfly PUF protecting IP on every FPGA / S. S. Kumar, J. Guajardo, R. Maes [et al.] // Proc. of the IEEE Intern. Workshop on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, USA, 09 June 2008. – Anaheim, 2008. – P. 67–70. – DOI: 10.1109/HST.2008.4559053.

6. Corner models: Inaccurate at best, and it only gets worst / C. C. McAndrew, I.-S. Lim, B. Braswell, D. Garrity // Proc. of the IEEE 2013 Custom Integrated Circuits Conf., San Jose, CA, USA, 22–25 Sept. 2013. – San Jose, 2013. – P. 1–4. – DOI: 10.1109/CICC.2013.6658428.

7. Ярмолик, В. Н. Двухмерные физически неклонируемые функции типа арбитр / В. Н. Ярмолик, А. А. Иванюк // Информатика. – 2023. – Т. 20, № 1. – С. 7–26. – DOI: 10.37661/1816-0301-2023-20-1-7-26.

8. Global interconnections in FPGAs: modeling and performance analysis / T. Mak, C. D'Alessandro, P. Sedcole [et al.] // Proc. of Intern. Workshop on System Level Interconnect Prediction, Newcastle, United Kingdom, 05–08 April 2008. – Newcastle, 2008. – P. 51–58. – DOI: 10.1145/1353610.1353621.

9. Karnik, T. An empirical model for accurate estimation of routing delay in FPGAs / T. Karnik, S.-M. Kang // Proc. of IEEE Intern. Conf. on Computer Aided Design (ICCAD), San Jose, CA, USA, 05–09 Nov. 1995. – San Jose, 1995. – P. 328–331. – DOI: 10.1109/ICCAD.1995.480136.

10. Иванюк, А. А. Конфигурируемый кольцевой осциллятор с управляемыми межсоединениями / А. А. Иванюк, В. Н. Ярмолик // Безопасность информационных технологий. – 2024. – Т. 31, № 2. – С. 121–133. – DOI: 10.26583/bit.2024.2.08.

11. Иванюк, А. А. Физически неклонируемые функции на базе управляемого кольцевого осциллятора / А. А. Иванюк, В. Н. Ярмолик // Безопасность информационных технологий. – 2023. – Т. 30, № 3. – С. 90–103. – DOI: 10.26583/bit.2023.3.06.

References

1. Chang Ch. H., Potkonjak M. (eds.). *Secure System Design and Trustable Computing*. Switzerland, Springer, 2016, 549 p. DOI: 10.1007/978-3-319-14971-4.

2. Hemavathy S., Bhaaskaran V. S. K. Arbiter PUF – a review of design, composition, and security aspects. *IEEE Access*, 2023, vol. 11, pp. 33979–34004. DOI: 10.1109/ACCESS.2023.3264016.

3. Maiti A., Schaumont P. Improved ring oscillator PUF: An FPGA-friendly secure primitive. *Journal of Cryptology*, 2011, vol. 24, pp. 375–397. DOI: 10.1007/s00145-010-9088-4.

4. Deng D., Hou S., Wang Z., Guo Y. Configurable ring oscillator PUF using hybrid logic gates. *IEEE Access*, 2020, vol. 8, pp. 161427–161437. DOI: 10.1109/ACCESS.2020.3021205.

5. Kumar S. S., Guajardo J., Maes R., Schrijen G.-J., Tuyls P. Extended abstract: The butterfly PUF protecting IP on every FPGA. *Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST), Anaheim, CA, USA, 09 June 2008*. Anaheim, 2008, pp. 67–70. DOI: 10.1109/HST.2008.4559053.

6. McAndrew C. C., Lim I.-S., Braswell B., Garrity D. Corner models: Inaccurate at best, and it only gets worst. *Proceedings of the IEEE 2013 Custom Integrated Circuits Conference, San Jose, CA, USA, 22–25 September 2013*. San Jose, 2013, pp. 1–4. DOI: 10.1109/CICC.2013.6658428.

7. Yarmolik V. N., Ivaniuk A. A. *2D physically unclonable functions of the arbiter type*. Informatika [*Informatics*], 2023, vol. 20, no. 1, pp. 7−26 (In Russ.). DOI: 10.37661/1816-0301-2023-20-1-7-26.

8. Mak T., D'Alessandro C., Sedcole P., Cheung P. Y. K., …, Luk W. Global interconnections in FPGAs: modeling and performance analysis. *Proceedings of International Workshop on System Level Interconnect Prediction, Newcastle, United Kingdom, 05–08 April 2008*. Newcastle, 2008, pp. 51–58. DOI: 10.1145/1353610.1353621.

9. Karnik T., Kang S.-M. An empirical model for accurate estimation of routing delay in FPGAs. *Proceedings of IEEE International Conference on Computer Aided Design (ICCAD), San Jose, CA, USA, 05–09 November 1995*. San Jose, 1995, pp. 328–331. DOI: 10.1109/ICCAD.1995.480136.

10. Ivaniuk A. A., Yarmolik V. N. *Configurable ring oscillator with controlled interc*onnections. Bezopasnost` informatsionnykh tekhnologiy [*IT Security (Russia)*], 2024, vol. 31, no. 2, pp. 121–133 (In Russ.). DOI: 10.26583/bit.2024.2.08.

11. Ivaniuk A. A., Yarmolik V. N. *Physically unclonable functions based on a controlled ring oscillator*. [*IT Security (Russia)*], 2023, vol. 30, no. 3, pp. 90–103 (In Russ.). DOI: 10.26583/bit.2023.3.06.

Информация об авторе

Иванюк Александр Александрович, доктор технических наук, профессор, профессор кафедры информатики, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: ivaniuk@bsuir.by

Information about the author

Alexander A. Ivaniuk, D. Sc. (Eng.), Prof., Prof. of Computer Science Department, Belarusian State University of Informatics and Radioelectronics.
E-mail: ivaniuk@bsuir.by