http://dx.doi.org/10.35596/1729-7648-2023-21-3-56-62

Оригинальная статья
Original paper

УДК 681.324

АВТОМАТИЧЕСКАЯ БАЛАНСИРОВКА ПУТЕЙ ФИЗИЧЕСКИ НЕКЛОНИРУЕМОЙ ФУНКЦИИ ТИПА «АРБИТР»

А. Ю. ШАМЫНА, А. А. ИВАНЮК

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

Поступила в редакцию 10.02.2023

Аннотация. Рассмотрены особенности построения на базе программируемых логических интегральных схем физически неклонируемых функций типа «арбитр» (АФНФ). Обозначена проблема асимметрии пар путей АФНФ, отмечено негативное влияние данного явления на их характеристики. Приведено описание времяизмерительной системы на базе схемы кольцевого осциллятора, используемой для анализа временных характеристик путей АФНФ. Предложена методика автоматической балансировки задержек распространения сигнала через пути АФНФ на основе расчета корректирующего значения. Экспериментально подтверждена состоятельность методики балансировки исходя из улучшения характеристик АФНФ после ее применения. Представлено схематическое решение данной методики, которое может лечь в основу разработки схемы автокоррекции задержек через пути АФНФ с различным уровнем автономности.

Ключевые слова: физическая криптография, физически неклонируемые функции типа «арбитр», кольцевой осциллятор, автоматическая балансировка, программируемые логические интегральные схемы.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Шамына, А. Ю. Автоматическая балансировка путей физически неклонируемой функции типа «арбитр» / А. Ю. Шамына, А. А. Иванюк // Доклады БГУИР. 2023. Т. 21, № 3. С. 56–62. http://dx.doi.org/10.35596/1729-7648-2023-21-3-56-62.

AUTOMATIC BALANCING OF “ARBITER” PHYSICAL UNCLONABLE FUNCTION PATHS

ARTSIOM YU. SHAMYNA, ALEXANDER A. IVANIUK

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Submitted 10.02.2023

Abstract. The features of building on the basis of programmable logic integrated circuits of “arbiter” physical unclonable functions (APUF) are considered. The problem of asymmetry of pairs of APUF paths is indicated and the negative impact of this phenomenon on their characteristics is noted. A time measuring system based on a ring oscillator scheme, which is used to analyze the time characteristics of APUF paths, is described. A method for automatic balancing of signal propagation delays through the APUF paths based on the calculation of the corrective value is proposed. The consistency of the proposed balancing technique is experimentally confirmed based on the improvement in the characteristics of the APUF after its implementation. A digital scheme of this technique is presented, which can form the basis for the development of a delay auto-correction scheme through APUF paths with different levels of autonomy.

Keywords: physical cryptography, “arbiter” physical unclonable functions, ring oscillator, automatic balancing, programmable logic integrated circuits.

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

For citation. Shamyna A. Yu., Ivaniuk A. A. (2023) Automatic Balancing of “Arbiter” Physical Unclonable Function Paths. *Doklady BGUIR*. 21 (3), 56–62. http://dx.doi.org/10.35596/1729-7648-2023-21-3-56-62 (in Russian).

Введение

Применение физически неклонируемых функций (ФНФ) [1, 2] является одним из перспективных направлений развития физической криптографии. Решения на их основе задействованы в областях защиты цифровых устройств от нелегального копирования и использования, протоколах аутентификации, проверки подлинности, а также как источник случайности в различного рода генераторах случайных чисел.

Особое место среди видов ФНФ занимают ФНФ типа «арбитр» (АФНФ) [3]. Их принцип работы основывается на различиях в прохождении сигнала через симметричные пути цифровых устройств. Зачастую условие симметрии пары путей является обязательным для функционирования АФНФ. Однако на практике данное условие сложно соблюсти при реализации АФНФ на таких популярных платформах, как программируемые логические интегральные схемы (ПЛИС). В статье предлагается подход к синтезу схем АФНФ, основанный на корректировке заведомо несимметричных пар путей, что позволяет улучшить основные характеристики АФНФ.

Анализ задержек через пути физически неклонируемых функций типа «арбитр»

Для оценки необходимости коррекции проведены экспериментальные исследования путей классической схемы АФНФ, построенных на последовательно соединенных n парах мультиплексоров [3]. С целью измерения значений задержек распространения сигналов через пути АФНФ была спроектирована и реализована на плате быстрого прототипирования экспериментальная установка (рис. 1), содержащая времяизмерительную систему на базе схемы кольцевого осциллятора.

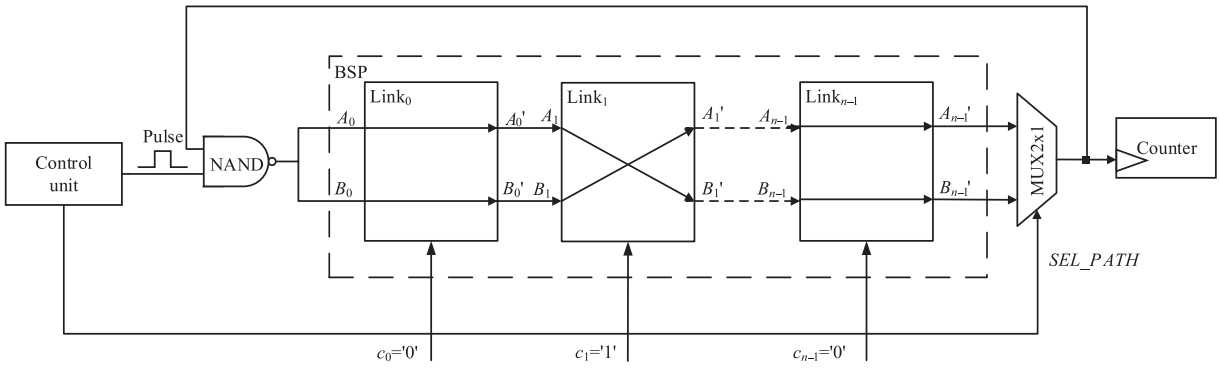


Рис. 1. Схема времяизмерительной системы на базе кольцевого осциллятора для классической схемы неклонируемых функций типа «арбитр»
Fig. 1. Scheme of a time measuring system based on a ring oscillator for a classical scheme of “arbiter” physical unclonable functions

Структура эксперимента аналогична схеме, описанной в [4]. Схема содержит блок управления Control unit, элемент NAND, обеспечивающий управление работой схемы в режиме осциллятора, а также исследуемый блок симметричных путей (БСП) BSP, используемый в классической АФНФ. БСП состоит из последовательно соединенных звеньев Link_i, $i \in [0, n–1]$, каждое из которых обеспечивает прямую либо перекрестную передачу сигнала с уникальной задержкой с входов A_i и B_i на выходы A_i' и B_i' соответственно в зависимости от значения разряда $c_i \in \{0, 1\}$ запроса C. Таким образом обеспечивается функционирование пары путей A и B, которые будут обладать уникальной конфигурацией для каждого значения запроса. Для подсчета импульсов, генерируемых схемой в режиме осцилляции, применяется двоичный синхронный счетчик. Обозначим задержку распространения через пути A и B как Δ_A и Δ_B соответственно. Двухвходовой

мультиплексор MUX2x1 используется для выбора активного пути на основе значения селектирующего сигнала *SEL_PATH*. Разницу между задержками прохождения тестового сигнала двух путей для одного запроса определим как $\Delta(\Delta_A, \Delta_B)$. Перевод значения счетчика $Count_{Path}$ в величину задержки Δ_{Path}, где $Path \in \{A, B\}$, для каждого измерения осуществляется по формуле

$$\Delta_{Path} = \frac{MW}{Count_{Path}}, \tag{1}$$

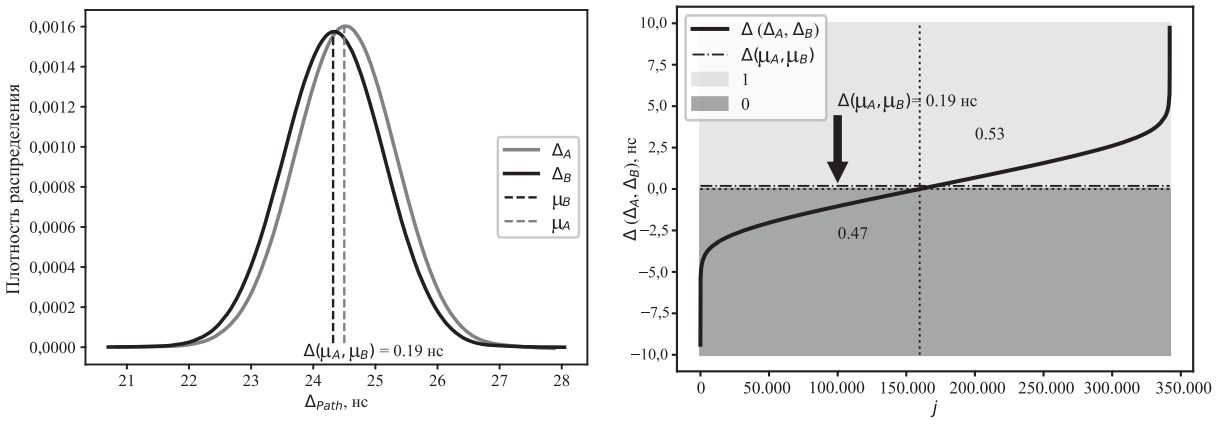
где MW – окно измерения.

Для оценки временного распределения задержек для пути используется оценка среднеарифметического значения задержек, которое определяется по формуле

$$\mu_{Path} = \frac{\sum_{k=0}^{N-1} \Delta_{Path}(C_k)}{N}, \tag{2}$$

где N – количество запросов; C_j – некоторый фиксированный запрос, $j \in [0, N-1]$ – порядковый номер запроса.

Эксперимент проводили для пары путей АФНФ с количеством звеньев $n = 64$. Всего было подано $N = 4 \cdot 10^6$ запросов, созданных с использованием генератора М-последовательности на базе LFSR. Эксперимент осуществляли на плате быстрого прототипирования Digilent Nexys 4 для четырех копий АФНФ на одном кристалле с ПЛИС Artix-7 xc7a100t csg324-1. Индексы копий АФНФ определяли как $d \in [0, D-1]$. Временное окно измерений $MW = kP_{SYS\_CLK} = 0{,}384$ мс, где k – коэффициент масштабирования (принимали $k = 38\,400$), P_{SYS_CLK} – период системного синхросигнала, $P_{SYS\_CLK} = 10$ нс. Результаты измеренных задержек Δ_A и Δ_B одной из копий АФНФ с индексом $d = 0$ на одном кристалле представлены на рис. 2 и в табл. 1.



a *b*

Рис. 2. Временное распределение измеренных задержек для схемы физически неклонируемых функций типа «арбитр» с $n = 64$: *a* – плотность распределения значений задержек; *b* – разница задержек
Fig. 2. Time distribution of the measured delays for the "arbiter" physical unclonable functions scheme with $n = 64$: *a* – distribution density of delay values; *b* – delay difference

Таблица 1. Временные характеристики путей *A* и *B* для четырех копий физически неклонируемых функций типа «арбитр»
Table 1. Time characteristics of "arbiter" physical unclonable functions paths *A* and *B* for four copies

d	μ_A	μ_B	$\Delta(\mu_A, \mu_B)$, нс
0	24,46229	24,27132	0,19097
1	23,26062	23,26379	–0,00317
2	24,99607	25,08964	–0,09357
3	22,83252	22,90313	–0,07061

Как видно из рис. 2, графики временных распределений задержек для двух путей копий АФНФ сдвинуты относительно друг друга во временной области, что может быть выражено как разница между средними значениями задержек для двух путей μ_A и μ_B соответственно. Этот факт подтверждается и данными табл. 1. Наличие такого сдвига свидетельствует об асимметрии построенных путей. Связано это, прежде всего, с реализацией рассматриваемой схемы на ПЛИС и ее автоматизированным синтезом. Такая особенность может привести к ухудшению характеристик АФНФ.

Балансировка путей физически неклонируемых функций типа «арбитр»

Методология построения и использования АФНФ сводится к определению из пары пути, который при некотором запросе обладает большей (или меньшей) задержкой прохождения тестового импульса и выработки на основе этого бита ответа R, где $R \in \{0,1\}$. Аналитически эту процедуру можно свести к определению значения $\Delta(\Delta_A(C_j), \Delta_B(C_j))$. Таким образом, значение бита ответа R будет соответствовать знаку рассчитанной разницы $\Delta(\Delta_A(C_j), \Delta_B(C_j))$. При таком подходе важны не абсолютные значения задержек, а разница между ними. Поэтому при непосредственном их измерении можно произвести процедуру коррекции, включающую предварительное вычисление средних значений задержки для каждого пути μ_A и μ_B и определение корректирующего значения $\Delta(\mu_A, \mu_B)$. Затем полученная величина используется для коррекции каждого измерения [4]. Одним из способов оценки случайности вырабатываемых ответов ФНФ является расчет метрики единообразия *Uniformity*, которая выражает отношение нулевых и единичных ответов ФНФ. В статье данная метрика применяется в нормализированном к единичному значению виде согласно формуле

$$Uniformity = 1 - \left| \frac{|R_0| - |R_1|}{N} \right|, \tag{3}$$

где $|R_0|$, $|R_1|$ – мощность множеств ответов ФНФ $R = 0$ и $R = 1$ соответственно.

Рассчитанная характеристика единообразия ответов АФНФ составила для $d = 0$ $Uniformity = 0{,}8$. Такое значение может являться неудовлетворительным для большинства приложений, где используются ФНФ. С целью проверки данного предположения вычисляли средние значения для каждого пути, причем при расчете среднего использовалось различное число измерений F. Затем они были пересчитаны с учетом коррекции величины метрики *Uniformity* для разных вариантов корректирующего значения (рис. 3).

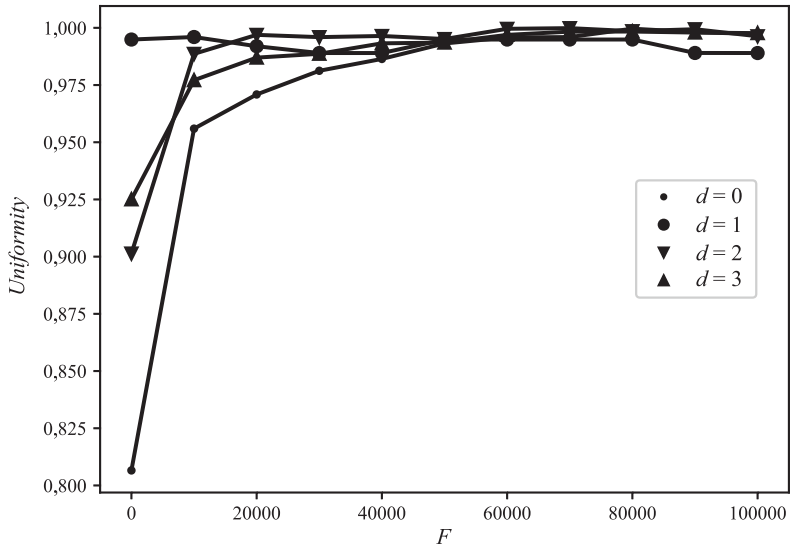
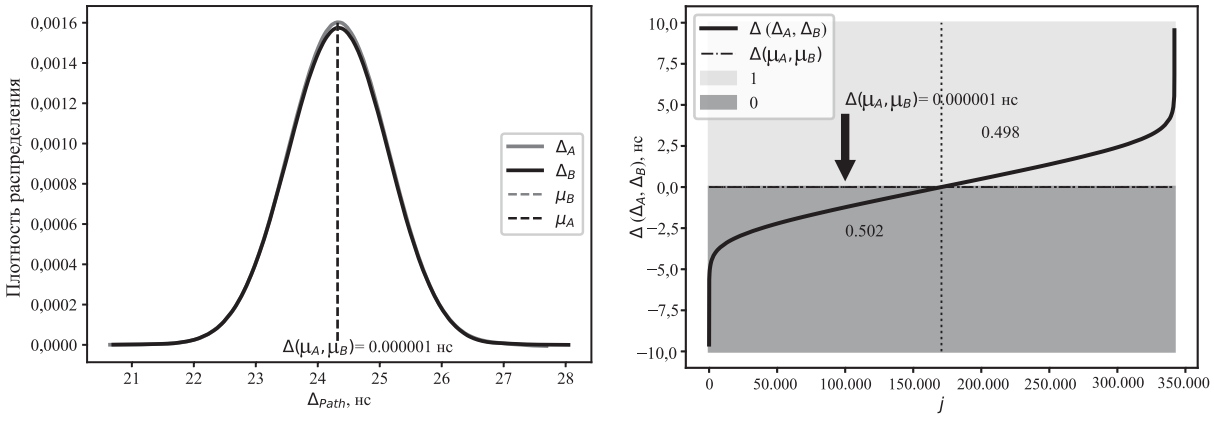


Рис. 3. Зависимость метрики от количества измерений
для расчета среднего значения физически неклонируемых функций типа «арбитр» с $n = 64$
Fig. 3. Dependence of the metric on the number of measurements
to calculate the average value for the “arbiter” physical unclonable functions scheme with $n = 64$

Как видно из рис. 3, при расчете корректирующей величины от большего значения F и дальнейшей коррекции всех измерений эксперимента улучшается характеристика единообразия *Uniformity*. График временного распределения полученных задержек с учетом коррекции представлен на рис. 4.



a *b*

Рис. 4. Временное распределение измеренных задержек с применением коррекции для схемы физически неклонируемых функций типа «арбитр» с $n = 64$:
a – плотность распределения значений задержек; *b* – разница задержек

Fig. 4. Time distribution of the measured delays with correction applied for the "arbiter" physical unclonable functions scheme with $n = 64$:
a – distribution density of delay values; *b* – delay differences

С учетом полученных результатов можно предположить, что добиться приемлемого значения корректирующего коэффициента можно за сравнительно небольшое число измерений. Допустим, что искомым значением будет *Uniformity* = 0,99. Тогда для всех копий АФНФ эксперимента достаточно $5 \cdot 10^4$ измерений для расчета корректирующего коэффициента. Стоит также отметить, что значения коррекции для каждого конкретного экземпляра являются различными (табл. 1). Поэтому существует необходимость в разработке решения, которое позволит автоматически производить расчет значения для коррекции за приемлемое время.

В результате выбрали корректирующее значение, дающее наилучшую величину *Uniformity*, с которой были пересчитаны другие характеристики. Для расчета основных характеристик АФНФ эксперимент воспроизводили $E = 20$ раз на $M = 4$ идентичных платах. До и после коррекции значения характеристики межкристальной U_{cmp} уникальности [5] составили $U_{cmp} = 0{,}01$ и $U_{cmp} = 0{,}02$ соответственно. Значения внутрикристальной уникальности и стабильности в результате коррекции также были немного улучшены. Характеристики единообразия *Uniformity* приведены в табл. 2.

Таблица 2. Характеристики физически неклонируемых функций типа «арбитр»
Table 2. Characteristics of "arbiter" physical unclonable functions

d	*Uniformity*	
	до коррекции / before correction	после коррекции / after correction
0	0,80657	0,99589
1	0,99489	0,99599
2	0,90136	0,99957
3	0,92504	0,99837

Полученные результаты расчетных характеристик АФНФ демонстрируют улучшение после применения коррекции по предложенной методике балансировки. Это подтверждает состоятельность описанного подхода.

Схема балансировки путей физически неклонируемых функций типа «арбитр»

При использовании АФНФ с предложенной методикой балансировки путей можно выделить две стадии: подготовки и нормального функционирования. На стадии подготовки выполняются следующие действия:

– вычисление среднего значения задержек μ_A и μ_B для путей A и B за приемлемое время;

– формирование корректирующих значений $\Delta(\mu(Count_A), \mu(Count_B))$ как целочисленных разностей между средними целочисленными величинами соответствующих путей.

Вычисление средних $\mu(Count_{Path})$ и корректирующих $\Delta(\mu(Count_A), \mu(Count_B))$ значений в целочисленном домене не влияет на конечный результат, но менее затратно с точки зрения потенциальной аппаратурной реализации. Этап подготовки может выполняться как при запуске устройства, так и с определенной периодичностью в зависимости от условий использования. В свою очередь, для работы АФНФ в нормальном режиме необходимо внедрение в схему выработки ответа АФНФ *Comparison* (рис. 5) учета корректирующего значения в виде сложения со значением одного из счетчиков схемы на каждом измерении. Разрядность счетчика выбирается исходя из формулы вычисления корректирующего значения.

Методику балансировки путей АФНФ, описанную выше, целесообразно представить в виде схемного описания. Такой подход благодаря наглядности позволяет перейти не только к целиком аппаратурному решению, но и к комбинированному, где часть действий балансировки может быть перенесена на выполнение другими компонентами системы, в которой предполагается использование АФНФ. Схема выработки бита ответа ФНФ R основана на сравнении значений счетчиков $Count_A$ и $Count_B$, полученных в результате измерения количества импульсов, регистрируемых за фиксированное время работы схемы в режиме кольцевого осциллятора (рис. 5).

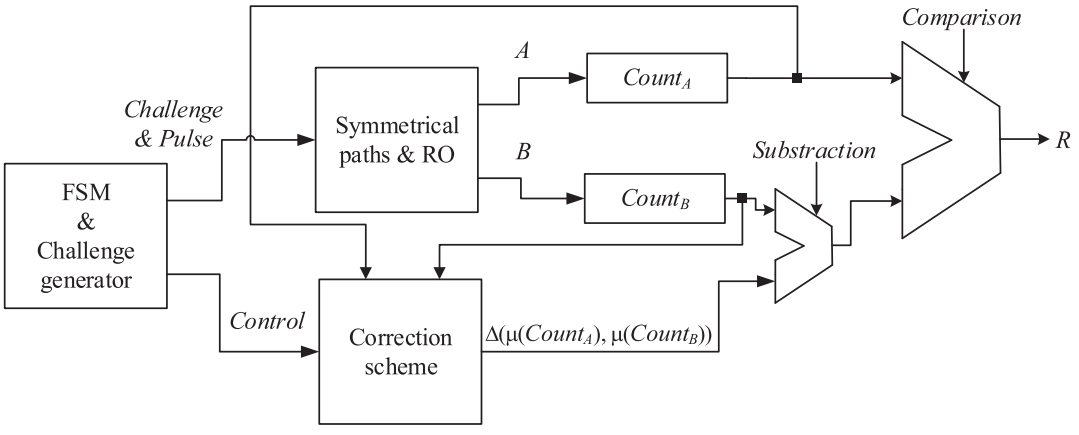


Рис. 5. Схема неклонируемых функций типа «арбитр» с коррекцией
Fig. 5. Scheme of “arbiter” physical unclonable functions with correction

Коррекция соотвествует операции вычитания корректирующих значений $\Delta(\mu(Count_A), \mu(Count_B))$ с выбранного значения счетчика для каждого измерения, выполняемой блоком *Substaction*. Расчет корректирующих значений $\Delta(\mu(Count_A), \mu(Count_B))$ соответствует вычислению разницы между средними значениями двух счетчиков. Количество итераций для измерения среднего $\mu(Count_{Path})$ может быть значительно уменьшено за счет генерации противоположных запросов с точки зрения результирующей разницы [6]. Конечный автомат FSM используется для управления режимом функционирования схемы. Генератор запросов Challenge generator применяется для подачи запросов, блок Correction scheme – для вычисления $\Delta(\mu(Count_A), \mu(Count_B))$ на этапе подготовки.

Выводы

1. Полученные результаты свидетельствуют о состоятельности предложенного подхода. Процедура балансировки путей физически неклонируемых функций типа «арбитр» может значительно улучшить их характеристики. Применение таких функций с автокоррекцией потенциально может решить проблему их использования при временной и эксплуатационной деградации кристаллов цифровых устройств. В совокупности данное решение позволяет избежать проблем физически неклонируемых функций типа «арбитр», связанных с применением в качестве арбитра схемы на базе триггеров различных модификаций.

2. В дальнейшем планируется продолжить исследования в данном направлении, прежде всего, с улучшением расчета корректирующего коэффициента и со снижением аппаратурных затрат.

Список литературы

1. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R Pappu. USA: Cambridge, Massachusetts Institute of Technology, 2001. 154 p.
2. Silicon Physical Random Functions / B. Gassend [et al.] // Proc. of the 9th ACM Conference on Computer and Communications Security, Novem. 2002. P. 148–160.
3. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. 2011. Т. 30, № 2. С. 92–103.
4. Шамына, А. Ю. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора / А. Ю. Шамына, А. А. Иванюк // Цифровая трансформация. 2022. Т. 28, № 1. С. 27–38. https://doi.org/10.35596/2522-9613-2022-28-1-27-38.
5. Ярмолик, В. Н. Физически неклонируемые функции типа арбитр с заведомо асимметричными парами путей / В. Н. Ярмолик, А. А. Иванюк // Доклады БГУИР. 2022. 20, № 4. С. 71–79.
6. Клыбик, В. П. Метод увеличения стабильности физически неклонируемой функции типа «АРБИТР» / В. П. Клыбик, С. С. Заливако, А. А. Иванюк // Информатика. 2017. № 1. С. 31–43.

References

1. Pappu R. (2001) *Physical One-Way Functions: PhD Thesis in Media Arts and Sciences*. USA, Cambridge, Massachusetts Institute of Technology. 154.
2. Gassend B., Clarke D., Van Dijk M., Devadas S. (2002) Silicon Physical Random Functions. *Proc. of the 9th ACM Conference on Computer and Communications Security, November.* 148–160.
3. Yarmolik V. N., Vashinko Y. G. (2011) Physical Unclonable Functions. *Informatika = Informatics*. 30 (2), 92–103 (in Russian).
4. Shamyna A. Yu, Ivaniuk A. A. (2022) Investigation of the Timing Parameters of the Arbiter-Based Physically Unclonable Function Using a Ring Oscillator. *Cifrovaya Transformaciya = Digital Transformation*. 28 (1), 27–38 (in Russian).
5. Yarmolik V. N., Ivaniuk A. A. (2022) Arbiter Physical Unclonable Functions with Asymmetric Pairs of Paths. *Doklady BGUIR*. 20 (4), 71–79 (in Russian).
6. Klybik V. P., Zalivako S. S., Ivanjuk A. A. (2017) Method of Increasing Stability Physically Non-Cloneable Function of "ARBITER" Type. *Informatika = Informatics*. (1), 31–43 (in Russian).

Вклад авторов

Шамына А. Ю. провел экспериментальные исследования, проанализировал и обобщил полученные результаты.

Иванюк А. А. осуществил постановку задачи для проведения исследования.

Authors' contribution

Shamyna A. Yu. conducted experimental studies, analyzed, and summarized the results.

Ivaniuk A. A. carried out the formulation of the problem for the study.

Сведения об авторах

Шамына А. Ю., магистр, ст. преп. Белорусского государственного университета информатики и радиоэлектроники

Иванюк А. А., д. т. н., доцент, профессор кафедры информатики, заведующий совместной учебной лабораторией «СК хайникс мемори солюшнс Восточная Европа» Белорусского государственного университета информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 25 941-60-45
E-mail: shamyna@bsuir.by
Шамына Артём Юрьевич

Information about the authors

Shamyna A. Yu., M. of Sci., Senior Lecturer at the Belarusian State University of Informatics and Radioelectronics

Ivaniuk A. A., Dr. of Sci. (Tech.), Associate Professor, Professor at the Computer Science Department, Head of the Joint Educational Laboratory "SK Hynix Memory Solutions Eastern Europe" of the Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 25 941-60-45
E-mail: shamyna@bsuir.by
Shamyna Artsiom Yur'evich