ЗАЩИТА ИНФОРМАЦИИ И НАДЕЖНОСТЬ СИСТЕМ
INFORMATION PROTECTION AND SYSTEM RELIABILITY

УДК 681.324
https://doi.org/10.37661/1816-0301-2022-19-4-27-41

Оригинальная статья
Original Paper

Построение и балансировка путей физически неклонируемой функции типа арбитр на FPGA

А. Ю. Шамына✉, А. А. Иванюк

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

Аннотация

Цели. Решается задача построения новой структуры путей физически неклонируемой функции типа арбитр (АФНФ) на FPGA (Field programable gate array), основанных на полном использовании внутренних ресурсов LUT-блоков (англ. Look up table), которые функционально являются повторителями. Актуальность исследования связана с бурным развитием средств физической криптографии. Также преследуется цель разработки способа устранения асимметрии путей АФНФ, связанной с особенностью синтеза подобных схем на FPGA.

Методы. Используются методы синтеза цифровых устройств, их параметрического моделирования и реализации на платах быстрого прототипирования. Для измерения внутренних задержек распространения сигналов через пути АФНФ применяется схема кольцевого осциллятора.

Результаты. Предложена новая структура базового элемента путей АФНФ с использованием двух функциональных повторителей. Продемонстрирована необходимость балансировки задержек путей АФНФ. Разработан способ устранения асимметрии распространения сигналов через пути АФНФ на базе управляемых линий задержки. Показаны недостатки использования в качестве схемы арбитра АФНФ классических подходов и необходимость их модификации.

Заключение. Предложенный подход к построению путей АФНФ показал свою состоятельность и перспективность. Экспериментально подтверждается улучшение характеристик АФНФ, построенных по предложенным способом, а также снижение аппаратурных затрат при их реализации по сравнению с классическими схемами АФНФ. Представляется перспективным дальнейшее развитие описанного подхода АФНФ, связанное прежде всего с усовершенствованием структуры арбитра.

Ключевые слова: физическая криптография, физически неклонируемые функции типа арбитр, симметричные пути, управляемые линии задержки, кольцевой осциллятор

Благодарности. Авторы выражают благодарность резиденту Парка высоких технологий компании SK Hynix Memory Solutions Eastern Europe за предоставленное оборудование для проведения экспериментальных исследований в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

Для цитирования. Шамына, А. Ю. Построение и балансировка путей физически неклонируемой функции типа арбитр на FPGA / А. Ю. Шамына, А. А. Иванюк // Информатика. – 2022. − Т. 19, № 4. – С. 27–41. https://doi.org/10.37661/1816-0301-2022-19-4-27-41

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Поступила в редакцию | Received 22.07.2022
Подписана в печать | Accepted 14.09.2022
Опубликована | Published 29.12.2022

Creating and balancing the paths of arbiter-based physically unclonable functions on FPGA

Artsiom Yu. Shamyna✉, Alexander A. Ivaniuk

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

Abstract
Objectives. The problem of constructing a new structure of paths of physically unclonable function of the arbiter type (APUF) on the FPGA is being solved, based on the full use of internal resources of LUT-blocks, which are functionally repeaters. The relevance of the study is associated with the rapid development of physical cryptography tools. Another goal is the developing a methodology for eliminating the asymmetry of the APUF paths associated with the peculiarity of the synthesis of such circuits on the FPGA.
Methods. The methods of synthesis of digital devices, their parametric modeling and implementation on rapid prototyping boards are used. A ring oscillator circuit is used to measure the internal propagation delays of signals through the APUF paths.
Results. A new structure of the basic element of APUF paths with the use of two functional repeaters is proposed. The necessity of balancing the delays of APUF paths is demonstrated. A technique has been developed to eliminate the asymmetry of signal propagation through APUF paths based on controlled delay lines. The disadvantages of classical approaches as an APUF arbitrator and the need for their modification are shown.
Conclusion. The proposed approach to build APUF paths has shown its viability and promise. An improvement in the characteristics of APUF constructed according to the proposed method, as well as a reduction in hardware costs during their implementation compared to classical APUF schemes, is experimentally confirmed. It seems promising to develop the described methodology for constructing the APUF to improve the structure of the arbiter.

Keywords: physical cryptography, arbiter-based physically unclonable functions, symmetrical paths, propagation delay line, ring oscillator

Acknowledgments. The authors express gratitude to the HTP resident of the "SK Hynix Memory Solutions Eastern Europe" company for the equipment provided for carrying out experiments within the framework of the joint laboratory with the Belarusian State Unitversity of Informatics and Radioelectronics.

For citation. Shamyna A. Yu., Ivaniuk A. A. *Creating and balancing the paths of arbiter-based physically unclonable functions on FPGA*. Informatika [*Informatics*], 2022, vol. 19, no. 4, pp. 27−41 (In Russ.).
https://doi.org/10.37661/1816-0301-2022-19-4-27-41

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

Введение. В настоящее время все большая роль отводится средствам физической криптографии, где одним из наиболее популярных направлений является изучение физически неклонируемых функций (ФНФ) [1]. Основополагающая идея ФНФ заключается в извлечении харак-

теристик, свойственных конкретной физической системе и являющихся уникальными и неповторяемыми, но при этом достаточно стабильными и удовлетворяющими определенным критериям при их многократном извлечении. Большинство ФНФ, реализованных в составе цифровых устройств, которые идентичны с точки зрения проектного описания и технологии изготовления интегральных схем, основаны на вариативности задержек распространения сигналов по фиксированным путям. Это свойство обусловлено естественными флуктуациями в материалах, используемых при производстве данных устройств, а также некоторым несовершенством производственного процесса.

Популярным схемотехническим решением, позволяющим на основе уникальности задержек распространения сигналов по топологически симметричным путям различных экземпляров одного устройства генерировать битовую последовательность для некоторого множества фиксированных запросов, является использование так называемых физически неклонируемых функций типа арбитр [2, 3].

Классическая схема АФНФ. В классической схеме АФНФ подразумевается наличие генератора тестового сигнала (ГТС), блока симметричных путей (БСП) и арбитра (АРБ). Схема арбитра позволяет определить очередность прохождения фронтов тестового импульса через блок симметричных путей и выработать на этой базе ответ R (рис. 1). В свою очередь, БСП представляет собой последовательно соединенные звенья (ЗВ), которые, как правило, строятся с помощью двух мультиплексоров с конфигурацией 2×1 и обеспечивают прямую либо перекрестную передачу двух тестовых сигналов в зависимости от значения разряда запроса.

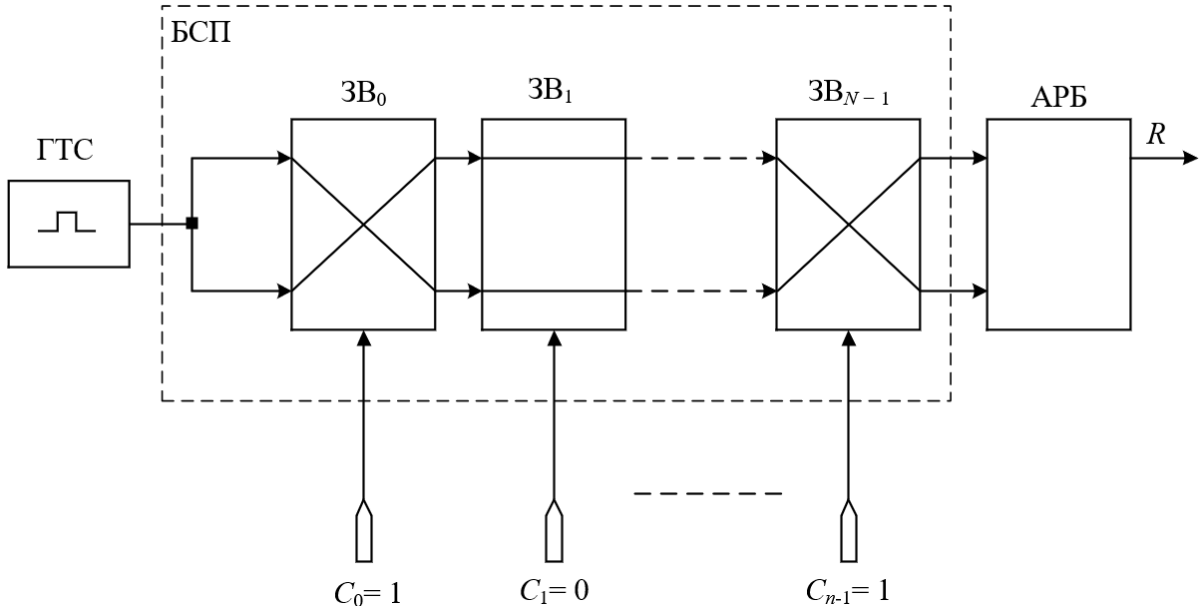
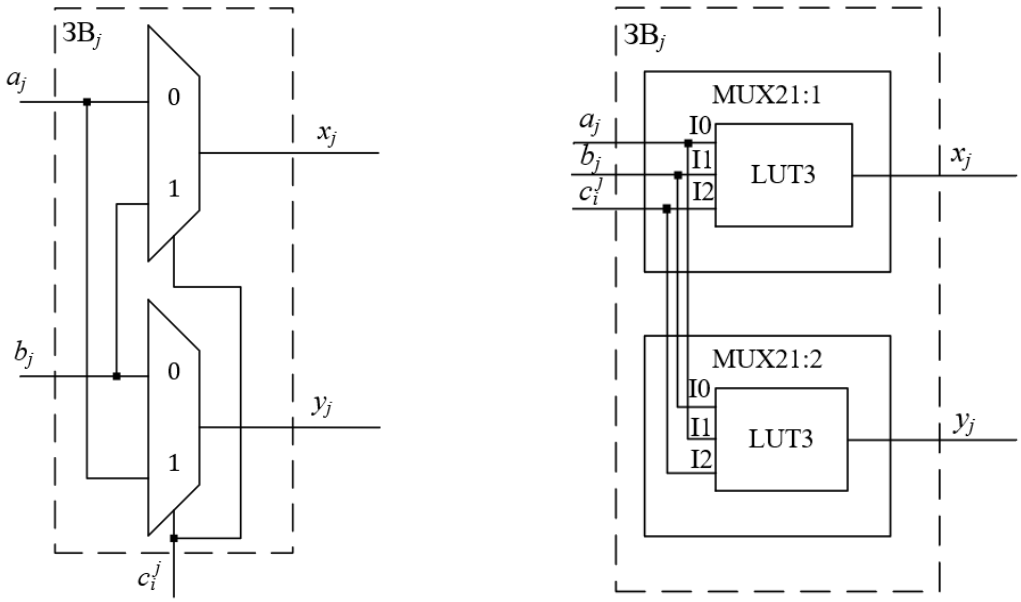


Рис. 1. Классическая схема АФНФ

Fig. 1. Classic APUF scheme

Общим подходом для построения звена $ЗВ_j$ является схема, состоящая из двух мультиплексоров (рис. 2, *a*). При реализации звена АФНФ на перепрограммируемых логических интегральных схемах типа FPGA будут использованы два блока LUT3 (рис. 2, *b*).

Вместе с тем при реализации АФНФ на современных FPGA, таких как Artix 7 фирмы Xilinx, возникает ситуация неполного использования ресурсов LUT-компонентов. Так, для реализации звена пути классической АФНФ требуются два LUT3, хотя фактически используются два технологических LUT6 и значительная часть их ресурсов остается незадействованной. Потенциально более полное использование ресурсов предоставляемых технологических компонентов FPGA может значительно сократить совокупные аппаратурные затраты при реализации АФНФ и улучшить их характеристики [4].



a) *b)*

Рис. 2. Реализация звена БСП классических АФНФ: *a)* RTL-схема; *b)* технологическая схема

Fig. 2. Implementation of the BSP link of classical APUF: a) RTL schematic; b) technology schematic

Схематично компонент LUT представляет собой память конфигурации и каскад мультиплексоров, обеспечивающий трансляцию единственного выбранного значения из этой памяти на выход схемы в зависимости от значений сигналов на адресных входах. На рис. 3 представлена реализация структурной схемы блока LUT4 FPGA фирмы Xilinx серии Spartan-3E, сконфигурированного для реализации одного мультиплексора классической АФНФ.

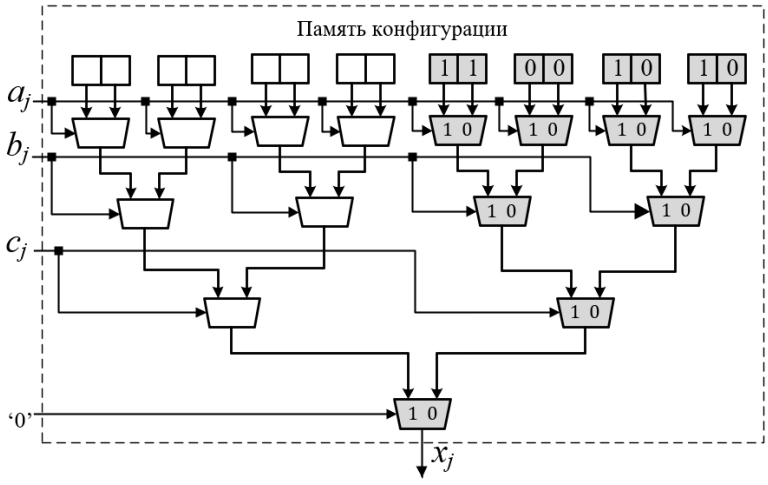


Рис. 3. Реализация мультиплексора звена БСП на LUT4

Fig. 3. Implementation of the BSP link multiplexer on LUT4

На рис. 3 видно, что ресурсы LUT4 задействованы лишь наполовину. Как правило, в стратегиях синтеза цифровых устройств не предусмотрено применение тех LUT-компонентов, которые уже были использованы, несмотря на то что значительная часть их ресурсов остается незадействованной, а при применении LUT-компонентов большей разрядности доля неиспользуемых ресурсов LUT-блоков становится еще более значительной. Так, в случае применения физического компонента LUT6 при реализации классической АФНФ для одного мультиплексора звена БСП будет израсходована лишь 1/8 доступных ресурсов.

Кроме того, как это было отмечено в работе [5], построение АФНФ на базе двух независимых путей может быть более предпочтительным с точки зрения статистических свойств, чем построение с помощью классического подхода, что обусловлено меньшей взаимной зависимостью задержек распространения сигналов через звенья пути.

Синтез предлагаемой архитектуры симметричных путей. Следует отметить, что при классическом подходе к построению АФНФ осуществляется неполное применение внутренних ресурсов LUT-блоков.

Идея более полного расхода доступных ресурсов LUT при реализации БСП АФНФ рассмотрена в работе [6]. В ней описан подход к построению БСП с использованием блоков функциональных мультиплексоров, копии которого размещены на одном LUT, а часть запроса, соответствующая одному звену БСП, отвечает за выбор не только прямой либо перекрестной передачи сигналов через звено, но и одной из двух копий мультиплексора, ее осуществляющей.

В настоящей работе в качестве звена БСП (рис. 4) предлагается задействовать схему двух функциональных повторителей, которые будут полностью расходовать ресурсы LUTN и обеспечивать 2^{N-1} уникальные трансляции в зависимости от $(N-1)$-разрядного запроса. Уникальность задержки сигнала при этом объясняется отличием пути прохождения сигнала непосредственно внутри самого LUT-блока в зависимости от значений сигналов на его адресных входах. Таким образом, при реализации, например, 128-разрядной АФНФ с применением компонентов LUT4 предложенная архитектура БСП позволяет сократить использование технологических LUT-компонентов в три раза при неизменной мощности множества запросов и ответов. Конфигурация LUT4, синтезированная по данной схеме, изображена на рис. 5.

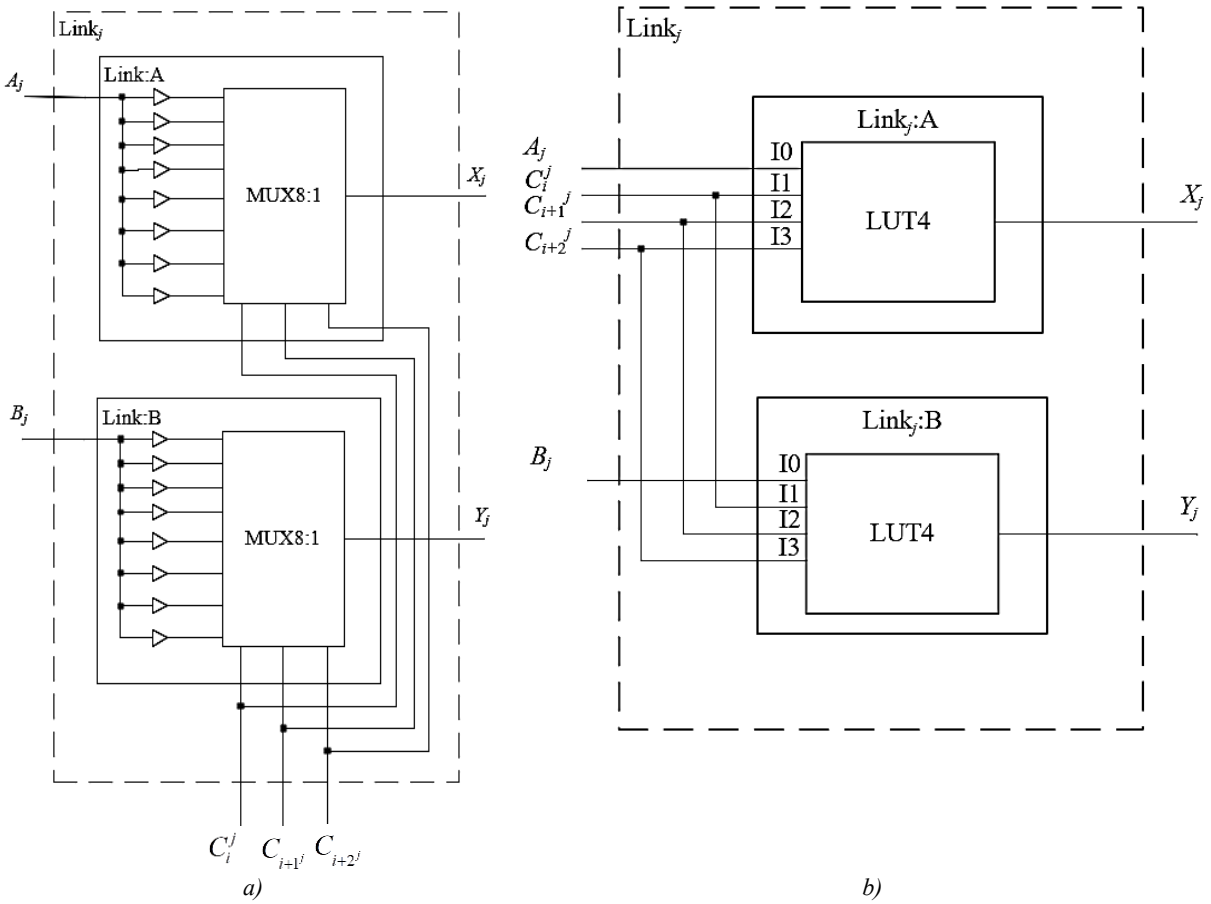


Рис. 4. Реализация одного звена БСП предложенной структуры: *a)* RTL-синтез; *b)* технологическая схема

Fig. 4. Implementation of one link of BSP of proposed structure: a) RTL schematic; b) technology schematic

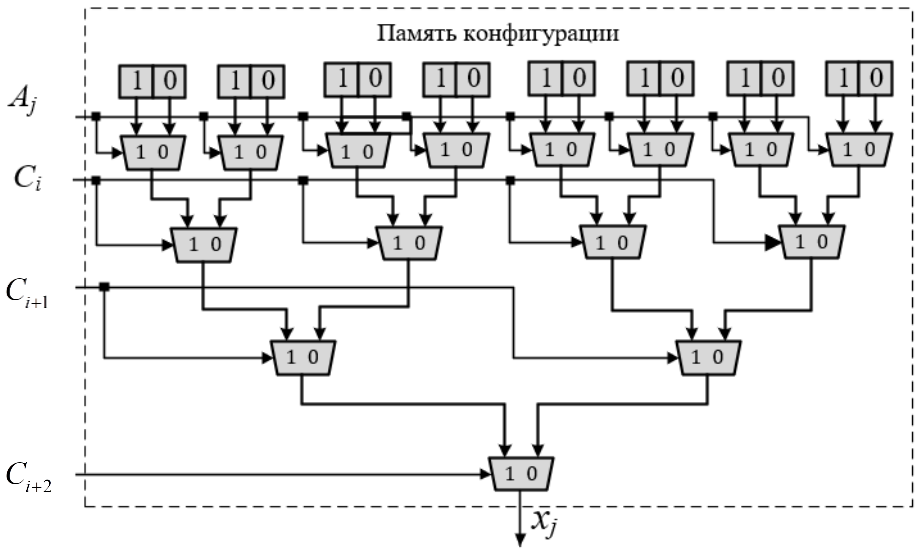


Рис. 5. Конфигурация LUT4 по предложенной структуре звена БСП

Fig. 5. LUT4 configuration according to proposed BSP link structure

Рассматриваемая схема полностью использует доступные ресурсы блока LUT и легко масштабируется под любую размерность LUT. Ее потенциальным недостатком является малое взаимное отличие проходимых сигналом путей при некоторых запросах. Так, при значениях векторов запроса $C_0C_1C_2 = 000$ и $C_0C_1C_2 = 100$ различие проходимых путей будет лишь в одном мультиплексоре. Данный факт требует дополнительных исследований.

Построение экспериментальной установки. Следует отметить важность построения симметричных путей АФНФ как источника для извлечения характеристик задержек распространения сигналов через пары путей, которые носят уникальный и случайный характер. В связи с асимметрией путей АФНФ могут значительно ухудшаться характеристики случайности и уникальности. Связано это прежде всего с тем, что ответ АФНФ в таком случае будет определен не уникальными свойствами временных задержек своего экземпляра, а асимметрией двух путей, обусловленной асимметричными межсоединениями их звеньев. Это может привести к тому, что в конечном итоге для всех изготовленных по идентичному проекту АФНФ при фиксированном запросе будет преобладать одинаковый ответ. Данная асимметрия межсоединений, как правило, не может быть перекрыта разницей задержек между конкретными экземплярами АФНФ на различных кристаллах и особенно для сравнительно небольшого количества звеньев путей АФНФ.

Ввиду неуправляемости автоматизированного синтеза на ПЛИС типа FPGA достаточно проблематично построить идеально симметричные пути с ее использованием. Получаемую при этом асимметрию можно условно разделить на асимметрию внутри конфигурационных блоков, которая в целом может быть нивелирована ручным размещением технологических компонентов, и на асимметрию межсоединений. Для минимизации асимметрии внутри конфигурационных блоков LUT-компоненты, которые являются составными звеньями БСП, были размещены особым образом [7]. Для этого использовались команды ограничения САПР Vivado LOC и BEL.

Для оценки временных характеристик распространения сигналов через симметричные пути АФНФ, построенные по предложенной структуре, ввиду невозможности временных измерений задержек внутри кристалла ПЛИС был использован подход на базе кольцевого осциллятора (КО), который подразумевает охват исследуемого пути отрицательной обратной связью. Данный подход требует наличия схемы управления режимом осцилляции, а также регистрации формируемой схемой импульсной последовательности (рис. 6).

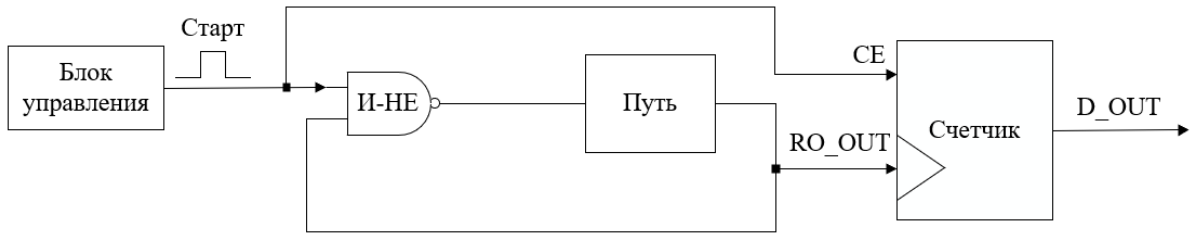


Рис. 6. Схема измерения задержек распространения сигналов на основе КО

Fig. 6. Scheme for measuring propagation delays based on QoS

Для достижения большей достоверности измерений было принято решение применить одну цепь обратной связи для измерения задержек двух симметричных путей. Для этого в последнем SLICE-блоке БСП был использован компонент F8MUX, выход которого соединен с цепью обратной связью, а два входа – с последними звеньями двух симметричных путей БСП. Таким образом, благодаря топологической и структурной схожести соединений внутри SLICE удалось свести к минимуму различия в измеряемых путях, непосредственно не относящиеся к ним.

Проектное описание экспериментальной установки, в которой помимо самостоятельно описанных модулей широко использовались IP-ядра и софт-процессор Microblaze, было создано в САПР Vivado 2018.2 с помощью языка VHDL. Эксперимент проводился на пяти идентичных платах быстрого прототипирования Digilent Nexys 4 с FPGA Artix 7. Общая схема эксперимента аналогична используемой в работе [8].

Экспериментальные исследования. Предложенная структура звена базируется на предположении об уникальности распространения задержек сигнала от входа до выхода LUT-блока в зависимости от значения запроса. Для реализации АФНФ на основе новой структуры звена БСП требуется обеспечить уникальность задержек в рамках как одного LUT-блока, так и нескольких LUT-блоков при соответствующих запросах. Для проверки предположения изначально был проведен следующий эксперимент. В матрице FPGA Artix 7 был выбран единственный SLICE-блок, в котором все доступные четыре LUT6-блока были сконфигурированы предложенным способом. Учитывая, что для измерения задержек была задействована схема КО, для увеличения достоверности измерений использовались фиксированная цепь обратной связи и схема измерений. Выбранный SLICE-блок был подключен к цепи измерений через выход внутреннего неконфигурируемого мультиплексора F8MUX. Также для коммутации LUT-блоков внутри SLICE были использованы два мультиплексора F7MUX. Данный способ измерения задержек для LUT-блоков, размещенных в одном SLICE-блоке, обоснован структурным подобием внутренних соединений внутри SLICE. Полученные таким способом экспериментальные данные должны максимально достоверно отражать уникальные задержки LUT6-блоков (рис. 7). Пять младших разрядов запроса *C* использовались как значения для адресных входов LUT-блоков, а два старших – как селектирующий сигнал для мультиплексоров, значения которых позволяют коммутировать выход одного из четырех LUT-блоков на выход SLICE.

Измеренные значения задержек распространения сигналов для всех LUT-компонентов SLICEL (X33Y90) представлены в табл. 1. Согласно данным табл. 1 задержки для каждого запроса являются уникальными. Значения среднеквадратического отклонения составили: $\sigma_{A6} = 0{,}004912384$, $\sigma_{B6} = 0{,}006597065$, $\sigma_{C6} = 0{,}001980557$, $\sigma_{D6} = 0{,}00171887$.

Затем эксперимент для выбранной конфигурации был повторен 100 раз на пяти кристаллах. Результаты продемонстрировали, что все полученные измерения задержек являются уникальными.

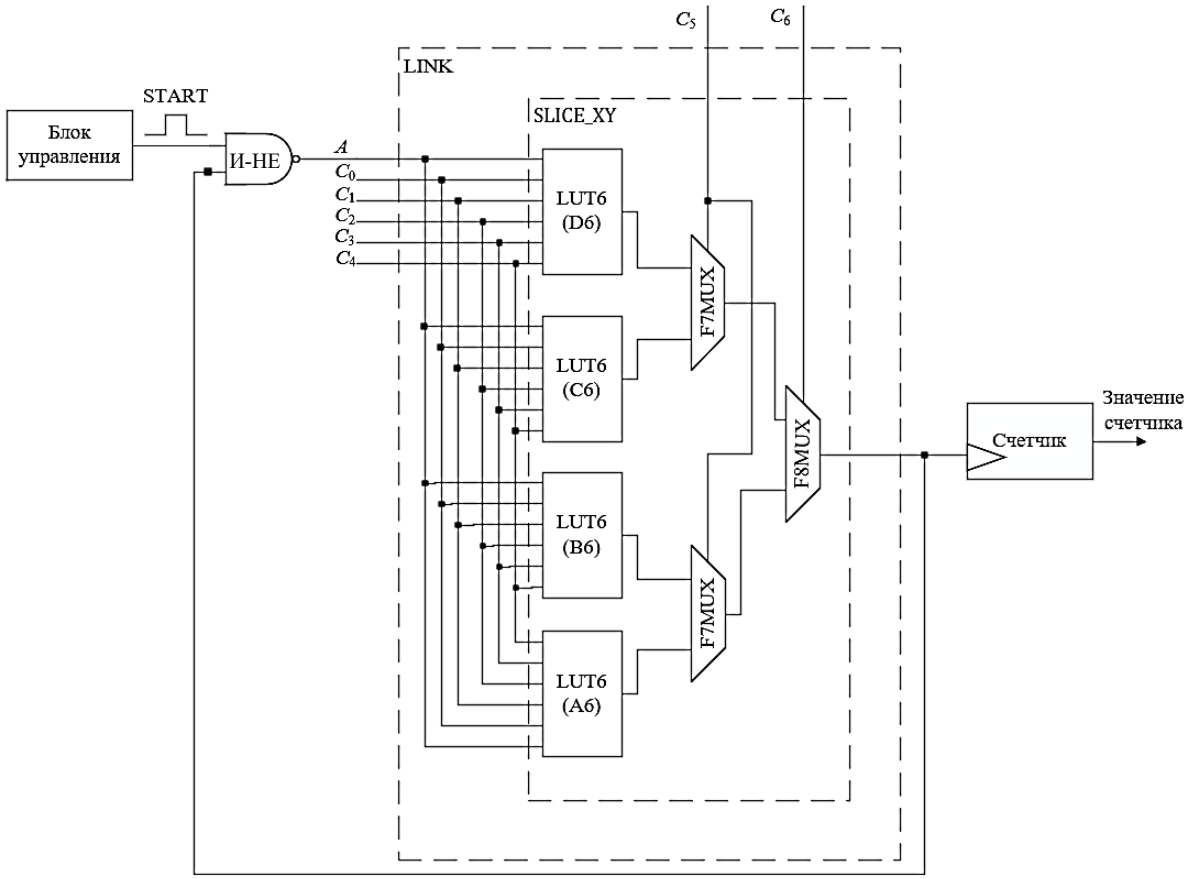


Рис. 7. Конфигурация SLICE-блока для эксперимента

Fig. 7. SLICE configuration for the experiment

Таблица 1

Значения задержек распространения сигналов через LUT-компоненты SLICEL, пс

Table 1

Propagation delay measurements through SLICEL LUTs, ps

Запрос *Challenge*	A6LUT	B6LUT	C6LUT	D6LUT
00000	1602,60	1086,39	1249,22	1548,14
00001	1601,53	1085,79	1249,08	1547,87
00010	1599,99	1084,92	1248,77	1548,07
00011	1603,18	1087,72	1248,64	1547,97
00100	1602,73	1087,74	1243,53	1549,38
00101	1601,51	1087,01	1243,35	1549,18
00110	1599,80	1087,12	1243,66	1552,14
00111	1602,46	1089,62	1243,42	1552,08
01000	1608,77	1081,38	1248,39	1550,58
01001	1607,54	1083,79	1248,48	1550,69
01010	1607,21	1084,76	1247,48	1551,10
01011	1611,55	1087,28	1247,43	1551,01
01100	1605,92	1088,65	1248,38	1550,23
01101	1609,22	1088,42	1248,17	1550,28
01110	1607,68	1083,32	1250,88	1551,86
01111	1607,48	1083,24	1250,65	1551,51
10000	1597,86	1069,96	1247,83	1547,60
10001	1597,86	1072,68	1247,79	1547,52

Окончание табл. 1

End of table 1

Запрос *Challenge*	A6LUT	B6LUT	C6LUT	D6LUT
10010	1594,46	1069,59	1247,36	1545,83
10011	1598,61	1073,16	1247,19	1545,58
10100	1595,90	1074,93	1247,22	1547,71
10101	1598,68	1075,67	1246,97	1547,70
10110	1597,31	1075,30	1244,97	1550,63
10111	1599,71	1078,72	1245,05	1550,72
11000	1592,80	1074,12	1249,15	1550,38
11001	1594,74	1073,70	1248,91	1550,49
11010	1595,77	1072,92	1247,42	1548,84
11011	1599,64	1073,27	1247,44	1548,54
11100	1599,53	1074,72	1247,25	1549,27
11101	1597,07	1074,80	1247,42	1549,07
11110	1596,70	1073,40	1249,47	1548,43
11111	1597,17	1074,21	1249,17	1548,23

Эксперимент был повторен и для других SLICE. Графики измеренных задержек для двух SLICE(X0Y198, X0Y1999) представлены на рис. 8.

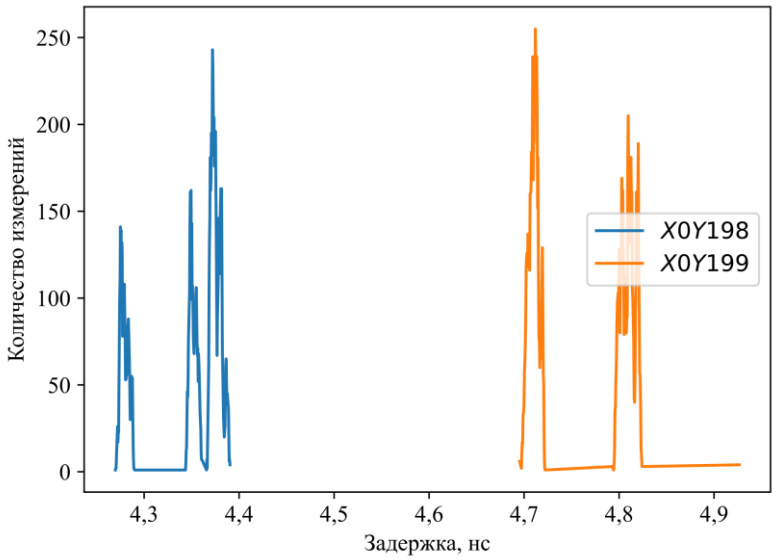


Рис. 8. Временное распределение задержек для двух SLICE

Fig. 8. Time distribution of delays for two SLICEs

Явный взаимный временной сдвиг графиков задержек для нескольких SLICE может говорить об отличиях в задержках как по линии отрицательной обратной связи схемы измерения, так и по линии распространения сигналов непосредственно в SLICE-блоках.

Полученные результаты демонстрируют целесообразность исследования задержек распространения сигналов через симметричные пути, построенные на базе звеньев предложенной структуры. Для этих целей было создано соответствующее VHDL-описание двух симметричных путей (рис. 9) для разрядности запроса $N = 64$. Для достижения максимальной симметричности путей в проектном описании LUT-блоки одного звена размещались в одном SLICE в соответствии с подходом, описанным в работе [7]. Генерирование запросов осуществлялось с помощью генератора М-последовательности на базе LFSR, всего было сгенерировано

$C = 10^6$ запросов. Следует также отметить, что, как и в предыдущих экспериментах, для измерений применялась фиксированная схема для двух путей. Результаты измерения временных задержек через симметричные пути для данного эксперимента представлены на рис. 10.

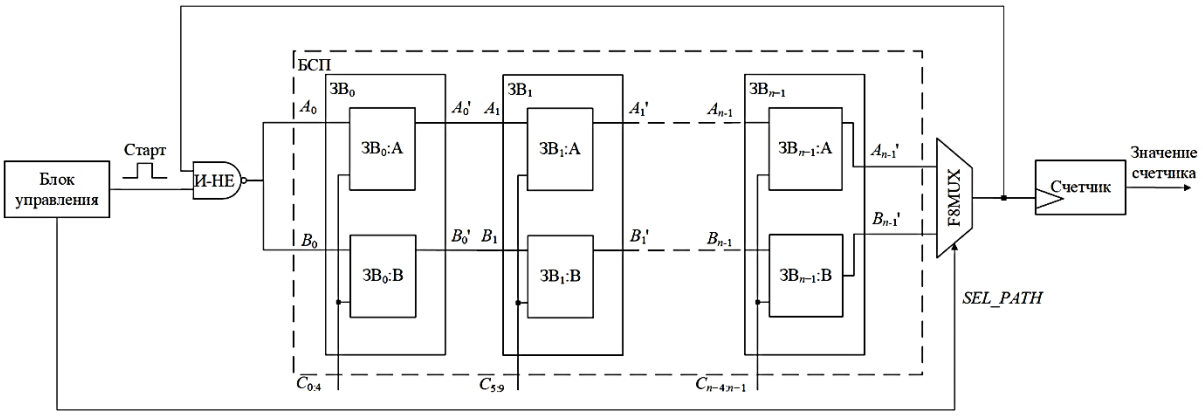


Рис. 9. Схема эксперимента

Fig. 9. Experiment scheme

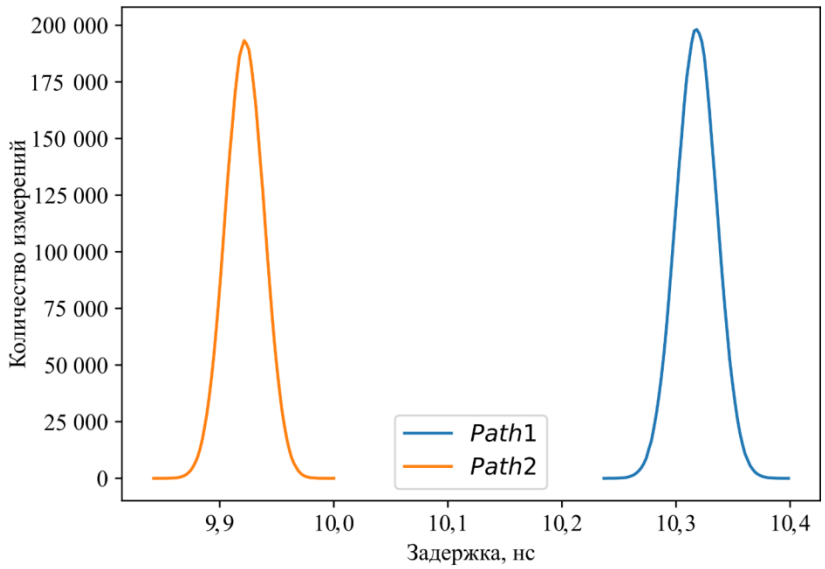


Рис. 10. Временное распределение задержек для двух симметричных путей при $N = 64$

Fig. 10. Time distribution of delays for two symmetrical paths with N = 64

Полученные результаты свидетельствуют о сдвиге по временной оси графиков задержек для двух симметричных путей и обусловлены прежде всего заведомой неуправляемостью автоматизированного построения межсоединений SLICE-блоков, а также уникальностью и неповторимостью значений задержек распространения сигналов через технологические компоненты FPGA на кристалле. Для построения АФНФ на их основе необходимо, чтобы временные задержки двух путей лежали в одном временном интервале. Достичь этого для текущей конфигурации можно при помощи управляемых линий задержек, базирующихся на последовательно соединенных мультиплексорах и встроенных между последним звеном БСП и потенциальным арбитром. Предлагаемое решение схемы балансировки представлено на рис. 11 и 12.

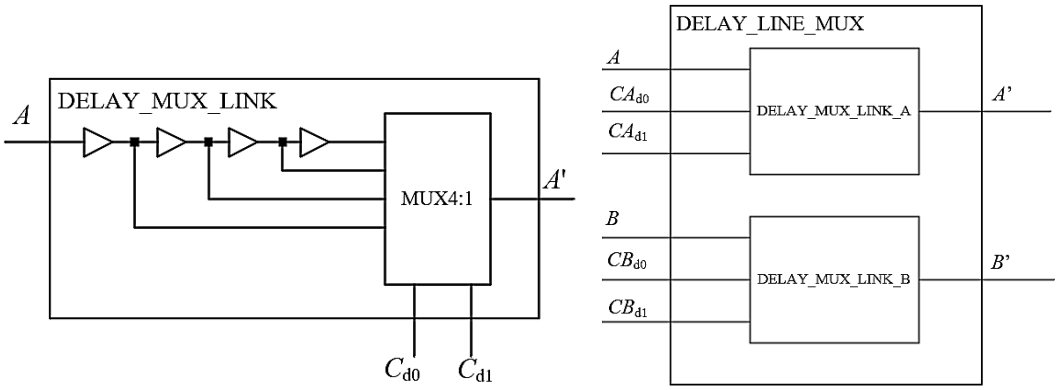


Рис. 11. Структура звена управляемой линии задержки

Fig 11. Propogation delay line link structure

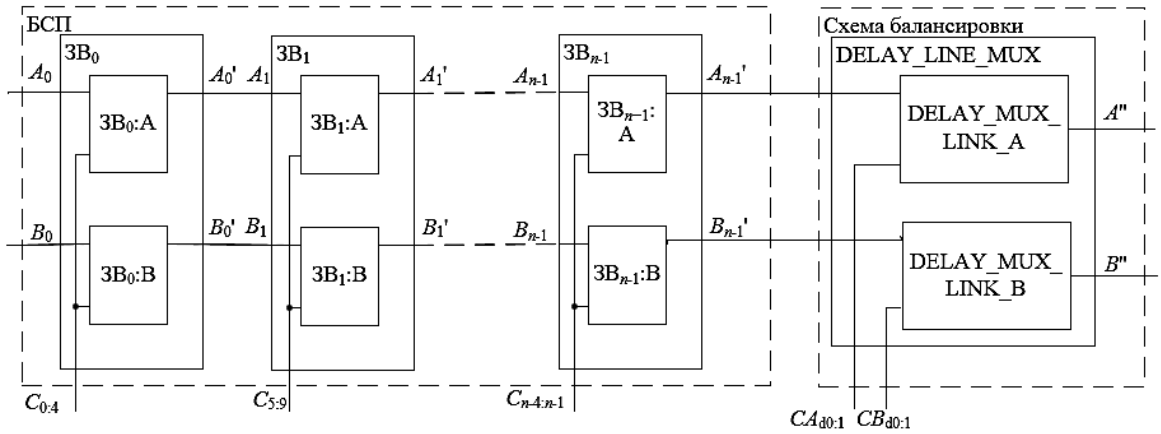


Рис. 12. Схема пары путей АФНФ с управляемой линией задержки

Fig. 12. Scheme of the pair of APUF paths with a propagation delay line

После построения схемы были подобраны такие значения управляющих сигналов $CA_{d0:1}$ и $CB_{d0:1}$ для двух линий задержек, при которых наблюдается минимальная разница между средними значениями задержек для двух построенных путей. Затем полученные значения управляющих сигналов были зафиксированы и с ними был повторен предыдущий эксперимент. Полученные результаты представлены на рис. 13.

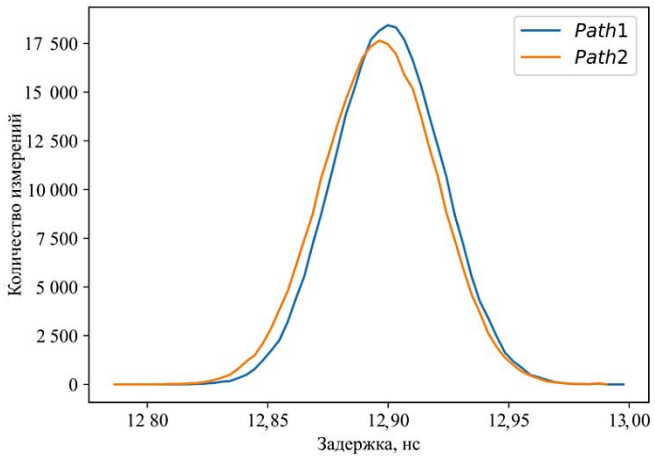


Рис. 13. Временное распределение задержек для двух симметричных путей при $N = 64$ с управляемой линией задержки

Fig. 13. Time distribution of delays for two symmetrical paths with N = 64 with controlled delay line

Вместе с тем, как показали исследования, крайне проблематично подобрать такие значения управляющих сигналов на линиях задержек выбранной конфигурации, чтобы измерения для двух путей лежали в одном временном интервале. Более того, смещения по временной оси измерений двух путей на каждом кристалле также различны, что еще более усложняет задачу сведения временных измерений в один интервал. Для решения этой задачи в схему балансировки была внедрена еще одна линия задержки DELAY_LINE_LUT, построенная на звеньях конфигурации, которая аналогична используемой в БСП для более тонкой подстройки фиксированных задержек. Из данных табл. 1 видно, что разброс значений задержек (разница между минимальным и максимальным значениями) для каждого звена составляет ~10 пс, также видна зависимость данной задержки от значения запроса. При этом межсоединения между SLICE остаются фиксированными и не зависят от запроса, как в линиях задержки DELAY_LINE_MUX, в которых различия значений задержек имеют больше, чем внутри LUT. В общем виде предлагаемая конфигурация АФНФ показана на рис. 14.

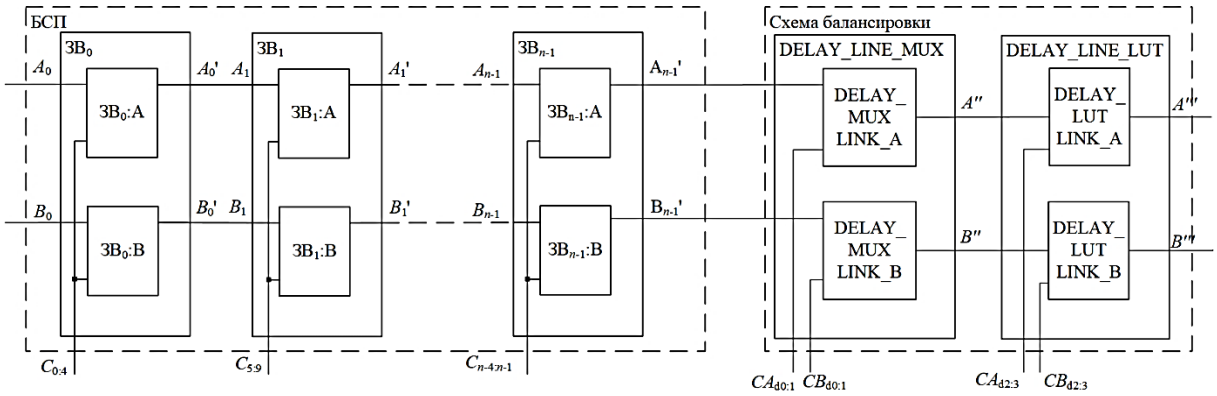


Рис. 14. Схема пары путей АФНФ с управляемой линией задержки

Fig. 14. Scheme of the pair of APUF paths with a propagation delay line

Стратегия подбора фиксированных значений управляющих сигналов для линий задержек состоит из нескольких шагов. Изначально подбирается такая пара управляющих сигналов для линий задержек, построенная на последовательно соединенных повторителях и мультиплексорах (DELAY_LINE_MUX), для которой разница между средними значениями для измерений двух путей минимальна. Затем данная пара управляющих значений фиксируется и выполняется подбор значений управляющих сигналов для линий задержек, построенных на базе LUT-компонентов, которые сконфигурированы аналогично звену БСП (DELAY_LINE_LUT). Критерием для определения лучшей комбинации управляющих сигналов служит разница между средними значениями. Процедура подбора значений для управления линиями фиксированных задержек выполняется индивидуально для каждого кристалла. После этого наиболее подходящие значения линий задержек фиксируются для проведения дальнейших измерений.

Распределения временных задержек для БСП размерности запроса $N = 64$ и график разниц измерений задержек для двух путей одного запроса показаны на рис. 15 и 16 соответственно.

Из полученных результатов следует, что в основном разницы задержек $\Delta(\text{Delay}_1, \text{Delay}_2)$ лежат в интервале, совпадающем с интервалом метастабильности для D-триггера, который чаще всего используется в качестве схемы арбитра АФНФ. Так, согласно документации (URL: https://china.xilinx.com/content/dam/xilinx/support/documents/data_sheets/ds181_Artix_7_Data_Sheet.pdf) для кристалла xc7a100tcsg324-1 время предустановки t_{setup} и время удержания thold составляют 0,07 и 0,12 нс соответственно для триггеров, расположенных в SLICEL. Таким образом, интервал метастабильности составляет $\Delta \in [-0{,}07; 0{,}12]$ нс. Данный факт требует дополнительной проработки схемы арбитра АФНФ для повышения стабильности ответов.

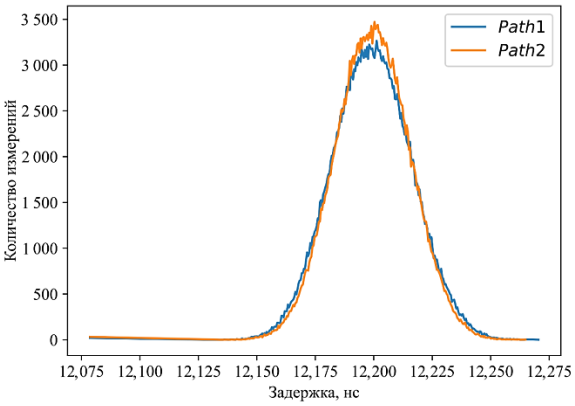


Рис. 15. Временное распределение задержек для конфигурации $N = 64$

Fig. 15. Time distribution of delays for two symmetrical paths with N = 64

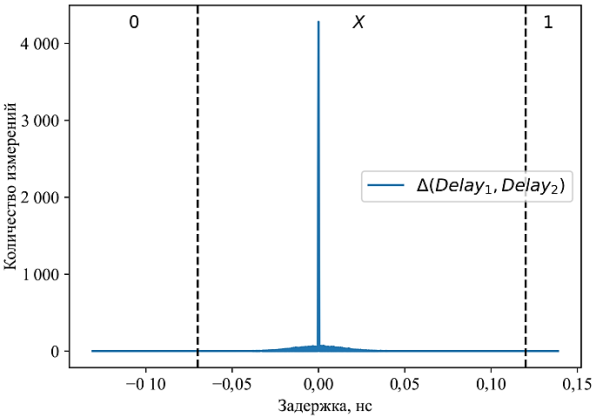


Рис. 16. Временное распределение разниц измерений задержек двух путей конфигурации $N = 64$

Fig. 16. Time distribution of delay measurement differences of two configuration paths N = 64

Также были рассчитаны важнейшие характеристики ФНФ стабильности S и межкристальной уникальности U_{cmp} [8] (табл. 2). Характеристика ФНФ стабильности S отражает свойство ФНФ сохранять идентичность ответа на фиксированный запрос при многократной его подаче. Под характеристикой межкристальной уникальности ФНФ U_{cmp} принято понимать долю таких запросов, при которых ответы для всех реализаций ФНФ на различных кристаллах будут уникальны. Аппаратурные затраты приведены в табл. 3.

Таблица 2
Характеристики АФНФ

Table 2
Characteristics of APUF

N	*S*	*Ucmp*	Доля ответов *Response rate*		
			X	0	1
Предлагаемая схема АФНФ *Proposed scheme APUF*					
32	0,88	0,5	0,02	0,46	0,52
64	0,94	0,48	0,01	0,48	0,51
128	0,96	0,53	0,01	0,49	0,5
Классическая АФНФ *Classical APUF*					
32	0,97	0,02	0,02	0,45	0,53
64	0,98	0,01	0,02	0,48	0,5
128	0,98	0,01	0,03	0,47	0,5

Таблица 3
Аппаратурные затраты, количество LUT

Table 3
Hardware utilization, LUTs

N	БСП *BSP*	Линии задержки *Delay line*	Общие затраты *Full utilization*	Классическая АФНФ *Classical APUF*
32	12	24	36	64
64	24	24	48	128
128	48	28	76	256

Из представленных данных видно, что, несмотря на определенные затраты на реализацию линий задержек, совокупные аппаратурные затраты значительно ниже, чем затраты на реализацию классической АФНФ с такой же разрядностью запросов. Кроме того, потенциально АФНФ, построенная по предложенной схеме, будет обладать значительно более высокими характеристиками уникальности и случайности по сравнению с классической схемой [6].

С увеличением числа звеньев БСП наблюдается улучшение стабильности, а также снижение количества измерений с равным значением задержки для одного запроса.

Заключение. В статье представлена новая архитектура звеньев БСП, базирующаяся на полном использовании ресурсов LUT-компонентов, которое подразумевает применение LUT-компонентов как функциональных повторителей. Описан подход снижения асимметрии двух путей БСП, основанный на ручном расположении LUT-компонентов. Для устранения асимметрии межсоединений SLICE-блоков предложен способ использования управляемых линий задержек. Однако значения различий временных задержек двух путей для фиксированного запроса демонстрируют невозможность применения в качестве арбитра для предложенной конфигурации симметричных путей D-триггера, который присутствует в классической схеме АФНФ, из-за нарушений условий предустановки и удержания входных сигналов.

В дальнейшем авторы планируют продолжить исследования по разработке конфигурации и архитектуры схемы арбитра, которая могла бы использоваться совместно с рассматриваемой в данной статье архитектурой БСП, а также исследования по изучению характеристик различных конфигураций управляемых линий задержек.

Вклад авторов. *А. Ю. Шамына* предложил идею построения и балансировки путей ФНФ с управляемой задержкой сигналов и провел экспериментальные исследования. *А. А. Иванюк* принял участие в обобщении и анализе полученных результатов.

Список использованных источников

1. Pappu, R. Physical One-Way Functions: PhD Thesis in Media Arts and Sciences / R. Pappu. – Cambridge : Massachusetts Institute of Technology, 2001. – 154 p.

2. Ярмолик, В. Н. Физически неклонируемые функции / В. Н. Ярмолик, Ю. Г. Вашинко // Информатика. – 2011. – № 2(30). – С. 92–103.

3. Иванюк, А. А. Физическая криптография и защита цифровых устройств / А. А. Иванюк, С. С. Заливако // Доклады БГУИР. – 2019. – № 2(120). – С. 50–58.

4. Yang, J. A low resource consumption Arbiter PUF improved switch component design for FPGA / J. Yang, X. Yu, R. Wei // J. of Physics: Conference Series. – 2022. – Vol. 2221. – P. 012011.

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. Иванюк, А. А. Синтез симметричных путей физически неклонируемой функции типа арбитр на FPGA / А. А. Иванюк // Информатика. – 2019. – Т. 16, № 2. – С. 99–108.

7. Secure lightweight obfuscated delay-based physicalunclonable function design on FPGA / M. H. Ishak [et al.] // Bulletin of Electrical Engineering and Informatics. – 2022. – Vol. 11, no. 2. – P. 1075–1083. https://doi.org/10.11591/eei.v11i2.3265

8. Шамына, А. Ю. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора / А. Ю. Шамына, А. А Иванюк // Цифровая трансформация. – 2022. – № 1(28). – С. 27–38.

References

1. Pappu, R. *Physical One-Way Functions: PhD Thesis in Media Arts and Sciences*. Cambridge, Massachusetts Institute of Technology, 2001, 154 p.

2. Yarmolik V. N., Vashinko Y. G. *Physical unclonable functions.* Informatika [*Informatics*], 2011, no. 2(30), pp. 92–103 (In Russ.).

3. Ivaniuk A. A., Zalivaka S. S. *Physical cryptography and security of digital devices.* Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioèlektroniki [*Reports of the Belarusian State University of Informatics and Radioelectronics*], 2019, no. 2(120), pp. 50–58 (In Russ.).

4. Yang J. , Yu X., Wei R. A low resource consumption Arbiter PUF improved switch component design for FPGA. *Journal of Physics: Conference Series*, 2022, vol. 2221, p. 012011.

5. Yarmolik V. N., Ivaniuk A. A. *Arbiter physical unclonable functions with asymmetric pairs of paths*. Doklady Belorusskogo gosudarstvennogo universiteta informatiki i radioèlektroniki [*Reports of the Belarusian State University of Informatics and Radioelectronics*], 2022, no. 20(4), pp. 71–79 (In Russ.).

6. Ivaniuk A. A. *Synthesis of symmetric paths of arbiter physically unclonable function on FPGA.* Informatika [*Informatics*], 2019, vol. 16, no. 2, pp. 99–108 (In Russ.).

7. Ishak M. H., Mispan M. S., Chiew W. Ya, Kamaruddin M. R., Korobkov M. A. Secure lightweight obfuscated delay-based physicalunclonable function design on FPGA. *Bulletin of Electrical Engineering and Informatics*, 2022, vol. 11, no. 2, pp. 1075–1083. https://doi.org/10.11591/eei.v11i2.3265

8. Shamyna A. Yu., Ivaniuk A. A. *Investigation of the timing parameters of the arbiter-based physically unclonable function using a ring oscillator*. Cifrovaya transformaciya [*Digital Transformation*], 2022, no. 1(28), pp. 27–38 (In Russ.).

Информация об авторах

Шамына Артем Юрьевич, магистр технических наук, старший преподаватель, Белорусский государственный университет информатики и радиоэлектроники.
E-mail: shamyna@bsuir.by

Иванюк Александр Александрович, доктор технических наук, доцент, профессор кафедры информатики, заведующий совместной учебной лабораторией «СК хайникс мемори солюшнс Восточная Европа», Белорусский государственный университет информатики и радиоэлектроники.
E-mail: ivaniuk@bsuir.by

Information about the authors

Artsiom Yu. Shamyna, M. Sc. (Eng.), Senior Lecturer, Belarusian State University of Informatics and Radioelectronics.
E-mail:shamyna@bsuir.by

Alexander A. Ivaniuk, D. Sc. (Eng.), Assoc. Prof., Prof. of Computer Science Department, Head of the Joint Educational Laboratory "SK Hynix Memory Solutions Eastern Europe", Belarusian State University of Informatics and Radioelectronics.
E-mail: ivaniuk@bsuir.by