ISSN 1816-0301 (Print)
ISSN 2617-6963 (Online)
УДК 004.312

Поступила в редакцию 14.01.2019
Received 14.01.2019

Принята к публикации 28.02.2019
Accepted 28.02.2019

Синтез симметричных путей физически неклонируемой функции типа арбитр на FPGA

А. А. Иванюк

Белорусский государственный университет
информатики и радиоэлектроники, Минск, Беларусь
E-mail: ivaniuk@bsuir.by

Аннотация. Физическая криптография является одним из актуальных направлений среди существующих методов защиты цифровых устройств от нелегального доступа. Схемотехнические решения, лежащие в основе физической криптографии, получили название цифровых физически неклонируемых функций (ФНФ), реализация которых обеспечивает уникальность, невоспроизводимость (неклонируемость) защищаемого цифрового устройства. Кроме того, ФНФ эффективны с точки зрения аппаратных ресурсов при их реализации. Существующие ФНФ типа арбитр основаны на синтезе конфигурируемых симметричных путей, каждое звено которых представляет собой пару двухвходовых мультиплексоров, обеспечивающих две конфигурации трансляции тестовых сигналов: прямую и перекрестную. Для построения на программируемой логической интегральной схеме (ПЛИС) типа FPGA одного звена необходимо применение двух встроенных LUT-блоков, обеспечивающих реализацию двух мультиплексоров, при этом ресурсы LUT-блоков используются не полностью. В статье предлагается новая архитектура звеньев симметричных путей ФНФ типа арбитр, позволяющая эффективно применять ресурсы LUT-блоков различных кристаллов FPGA.

Ключевые слова: физически неклонируемая функция, арбитр, симметричные пути, FPGA, LUT-блок

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

Synthesis of symmetric paths of arbiter physically unclonable function on FPGA

Alexander A. Ivaniuk

Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus
E-mail: ivaniuk@bsuir.by

Abstract. Physical cryptography is one of the current trends among the existing methods of protecting digital devices from illegal access. Circuit design solutions in physical cryptography are called digital physically unclonable functions (PUFs), which to be implemented ensure the uniqueness, non-reproducibility (non-cloning) of the protected digital device. In addition, PUFs should be efficient as hardware resources. The existing implementations of the arbiter PUF are based on the synthesis of configurable symmetric paths, when each link is a pair of two-input multiplexers providing two configurations of test signal translation: direct and cross. In order to build a single link on FPGA, it is necessary to use two built-in LUT-blocks, providing the implementation of two multiplexers, meanwhile the hardware resources of LUT-blocks are not fully utilized. The article presents a new architecture of symmetric paths of the arbiter PUF, allowing efficient use of hardware resources of LUT-blocks for various FPGA families.

Keywords: physically unclonable function, arbiter, symmetrical paths, FPGA, LUT-block

For citation. Ivaniuk A. A. Synthesis of symmetric paths of arbiter physically unclonable function on FPGA. *Informatics*, 2019, vol. 16, no. 2, pp. 99–108 (in Russian).

Введение. Обеспечение защиты цифровых устройств от несанкционированного использования, копирования и модификаций достигается различными методами, алгоритмами и техническими средствами. Среди них можно выделить относительно новое направление под общим названием физическая криптография, основу которого составляют так называемые физически неклонируемые функции [1]. Суть ФНФ заключается в извлечении уникальных физических характеристик из изготовленного цифрового устройства. Вариации технологических процессов изготовления интегральных схем вносят в их физическую структуру случайные, непредсказуемые изменения, делающие каждый экземпляр цифрового устройства уникальным, неповторимым и невоспроизводимым. Для извлечения уникальных характеристик устройство проектируют с добавлением специализированных цифровых схем, позволяющих по определенным запросам вырабатывать уникальные цифровые ответы, свойственные только данному экземпляру. В общем случае схемотехническая реализация ФНФ представляет собой схему с n цифровыми входами, на которые подается n-битный запрос C (Challenge) из 2^n возможных, и одним выходом ответа R (Response). Поведение подобной ФНФ-схемы можно описать случайной булевой функцией, осуществляющей отображение $\{0,1\}^n \rightarrow \{0,1\}$. Случайность такой функции обусловлена тем, что данное отображение множества запросов на множество ответов неизвестно до момента изготовления конкретного экземпляра устройства и зависит от случайных неконтролируемых вариаций всех составляющих технологического процесса.

Таким образом, множество всех возможных пар запрос-ответ ФНФ $CR_\alpha = \{c_0 r_0, c_1 r_1, ..., c_{2^n-1} r_{2^n-1}\}$ определяет уникальность конкретного экземпляра α цифрового устройства, а $r_i = PUF_\alpha(c_i)$, $i = \{0,1,...,2^n - 1\}$, определяет уникальную зависимость ответа r_i от запроса c_i.

Для возможности применения в физической криптографии ФНФ должна удовлетворять ряду критериев [2, 3]:

1. Аппаратурные затраты на реализацию ФНФ не должны превышать затраты на реализацию защищаемого устройства.

2. Сбор, хранение и анализ множества CR_α должны быть физически недостижимыми на современном оборудовании и за приемлемое время. ФНФ, обладающую таким свойством, называют сильной ФНФ, для которой параметр n является достаточно большим. Например, для n = 64 только для хранения одного множества R_α необходимо запоминающее устройство с информационной емкостью 16 эксабит, а время сбора всех значений R_α будет составлять более 580 лет с учетом времени отклика устройства, равного 1 нс.

3. Обладая информацией о паре запрос-ответ $c_i r_i$ для конкретного экземпляра устройства α, невозможно рассчитать, смоделировать либо иным математическим способом предсказать значение пары $c_j r_j$, $i \neq j$, или значения множества других пар. Если ФНФ удовлетворяет этому условию, то она считается случайной и непредсказуемой.

4. Для конкретного экземпляра устройства α множество ответов R_α^*, $|R_\alpha^*| < |R_\alpha|$, может быть неоднократно извлечено с высокой степенью надежности путем подачи соответствующего множества различных запросов C_α^*, $|C_\alpha^*| < |C_\alpha|$. Обладающая данным свойством ФНФ считается стабильной.

5. Для множества $\mathrm{A} = \{\alpha_0, \alpha_1, ..., \alpha_{m-1}\}$, $|\mathrm{A}| = m$, различных экземпляров цифрового устройства со встроенной схемой ФНФ, выполненных по единым технологическим нормам, должно соблюдаться следующее условие: $CR_{\alpha_0} \neq CR_{\alpha_1} \neq ... \neq CR_{\alpha_{m-1}}$. Данное условие может быть усилено

следующим образом: $R^*_{\alpha_0} \neq R^*_{\alpha_1} \neq ... \neq R^*_{\alpha_{m-1}}$ для соответствующего множества различных запросов $C^*_{\alpha_0} = C^*_{\alpha_1} = ... = C^*_{\alpha_{m-1}}$, $\left|C^*_{\alpha_0}\right| = \left|C^*_{\alpha_1}\right| = ... = \left|C^*_{\alpha_{m-1}}\right| = \lceil \log_2 m \rceil$. Если описанные условия выполняются, ФНФ считается уникальной.

При удовлетворении описанным критериям ФНФ может быть эффективно использована в качестве криптографического примитива для решения следующих задач [1]:

– неклонируемой идентификации цифровых устройств;
– надежной аутентификации цифровых устройств;
– генерирования случайных невоспроизводимых числовых последовательностей;
– реализации аппаратных хеш-функций;
– реализации аппаратных водяных знаков и отпечатков пальцев;
– защиты цифровых устройств от клонирования и модификаций.

Существует множество схемотехнических реализаций ФНФ для цифровых устройств [1, 2]: ФНФ типа арбитр, ФНФ кольцевых генераторов, ФНФ типа бабочка, ФНФ на основе запоминающих устройств и др. Практически все они основаны на измерении задержек распространения сигналов по путям, сформированным множеством последовательно подключенных цифровых элементов.

Одним из наиболее известных методов реализации ФНФ для цифровых устройств, основанных на измерении задержки распространения сигналов, является ФНФ типа арбитр (А-ФНФ) [4–8]. В отличие от других типов данная ФНФ является сильной и обладает приемлемыми аппаратурными затратами. Однако ее практическая реализация имеет ряд недостатков, которые пытаются устранить разработчики и исследователи в области физической криптографии. К основным проблемам А-ФНФ можно отнести слабую стабильность подмножества пар запрос-ответ и возможность построения ее точной модели по известному множеству пар CR^*_α, $\left|CR^*_\alpha\right| \ll \left|CR_\alpha\right|$ ввиду линейности ее схемотехнической структуры.

Рассмотрим особенности схемотехнического синтеза А-ФНФ для программируемых логических устройств типа FPGA.

Синтез классической схемы А-ФНФ на FPGA. Платы быстрого прототипирования цифровых устройств на основе кристаллов FPGA являются основной платформой для исследования, тестирования и верификации различных схемотехнических решений ФНФ [9, 10]. Рассмотрим обобщенную структуру А-ФНФ и результаты ее синтеза для FPGA.

Структура А-ФНФ состоит из трех основных блоков, последовательно соединенных между собой (рис. 1): генератора тестового сигнала (ГТС), блока симметричных путей (БСП) и блока арбитра (АРБ).

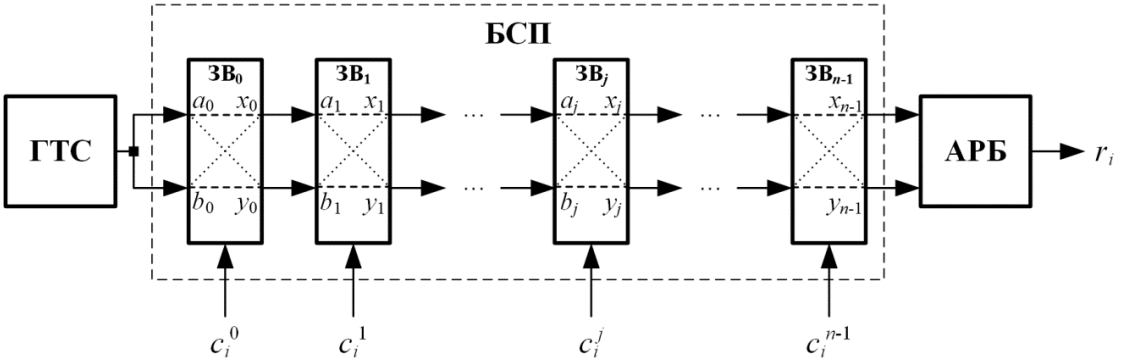


Рис. 1. Обобщенная структура А-ФНФ

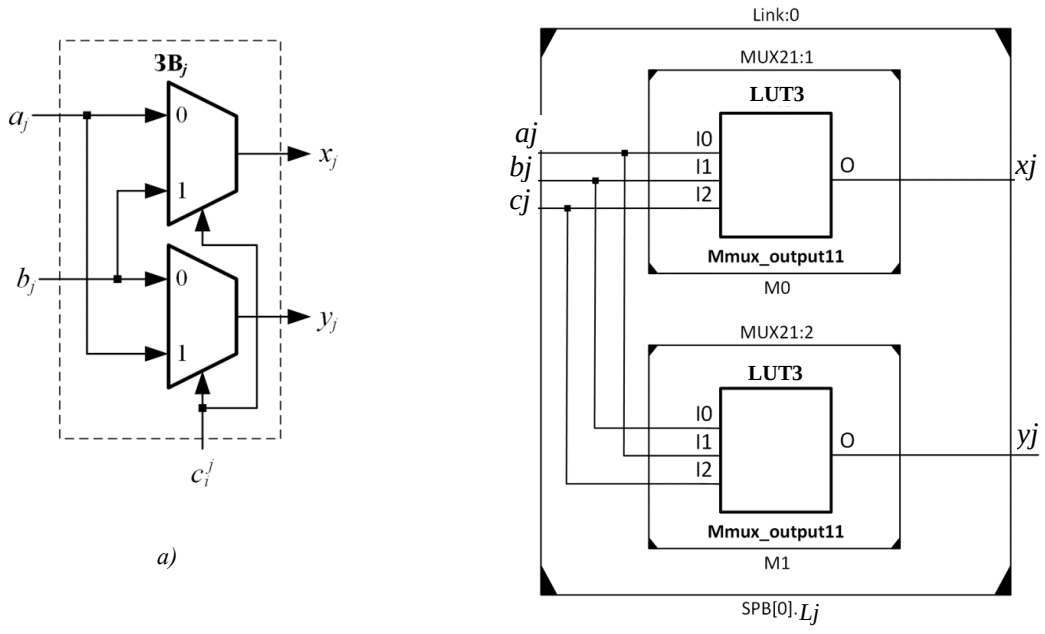
В свою очередь, БСП состоит из n звеньев (ЗВ_j), управляемых внешними сигналами $c_i^j \in \{0,1\}$, $j = \{0,1,2,...,n-1\}$, значения которых равны значениям соответствующих разрядов

подаваемого запроса c_i. Каждое звено $ЗВ_j$ имеет два входа a_j, b_j и два выхода x_j, y_j. В случае $c_j^i = 0$ происходит передача сигнала со входа a_j на выход x_j и со входа b_j на выход y_j. В противном случае, когда $c_j^i = 1$, передача сигнала осуществляется от входа a_j на выход y_j и от входа b_j на выход x_j. Соответственно, каждое звено имеет две конфигурации: прямой передачи сигналов и перекрестной передачи сигналов. Общее число последовательно соединенных звеньев *n* обеспечивает 2^n различных конфигураций путей прохождения двух копий тестового сигнала от блока ГТС до схемы АРБ. Назначение арбитра заключается в определении, какая из копий сигнала пришла раньше. Например, если сигнал, поступивший с выхода x_{n-1} на вход арбитра, оказался раньше сигнала y_{n-1}, то арбитр выработает на своем выходе значение $r_i = 1/0$. В противном случае арбитр установит на своем выходе значение $r_i = 0/1$.

В большинстве схемотехнических реализаций ГТС вырабатывает тестовый сигнал, в котором определяющим для работы всей схемы является его передний фронт [1]. В этом случае схема АРБ синтезируется с применением синхронного триггера D-типа, для которого на вход синхронизации поступает сигнал с выхода x_{n-1}, а на вход данных – с выхода y_{n-1} последнего звена. Кроме этого, некоторые разработчики применяют в качестве арбитра триггерные схемы с асинхронным сбросом и переустановкой, а также мультитриггерные схемы [5]. Основной проблемой применения перечисленных схемотехнических решений для синтеза схем АРБ является эффект метастабильности, негативно влияющий на стабильность всей схемы А-ФНФ. В работе [5] была предложена схема АРБ, позволяющая улучшить стабильность арбитра за счет обнаружения состояния метастабильности с дальнейшим его кодированием стабильным двухбитным двоичным значением.

При синтезе схемы сильной А-ФНФ с параметром $n \geq 8$ основные аппаратные затраты приходятся на БСП. Рассмотрим подробнее реализацию звеньев БСП.

Базовым подходом для реализации одного звена является схема, состоящая из двух мультиплексоров (рис. 2, *а*). Реализация данной схемы на ПЛИС типа FPGA будет выполнена с применением двух блоков LUT3, реализующих комбинационные схемы мультиплексоров с тремя входами.



а) *б)*

Рис. 2. Схемная реализация одного звена БСП: *а)* RTL-схема; *б)* технологическая схема

В свою очередь, блок LUT3 является моделью технологического элемента, позволяющей оценить реализацию комбинационной схемы на блоках LUT реального кристалла FPGA. Серийно выпускаемые кристаллы FPGA такого производителя, как Xilinx, имеют аппаратную структуру, способную реализовывать переключательные функции максимум от четырех либо шести аргументов в зависимости от архитектуры ПЛИС [11]. Структурно LUT-блоки состоят из памяти конфигурации и набора мультиплексоров, обеспечивающих трансляцию выбранного значения из этой памяти на свой единственный выход. Значение адреса памяти формируется из значений используемых управляемых входов мультиплексоров. Неиспользуемые входы при реализации малого числа аргументов принимают, как правило, константное значение 0.

На рис. 3 изображена структурная схема блока LUT FPGA фирмы Xilinx серии Spartan-3E [12], сконфигурированного для реализации одного мультиплексора с выходом x_j из схемы ЗВ_j (см. рис. 2, *а*).

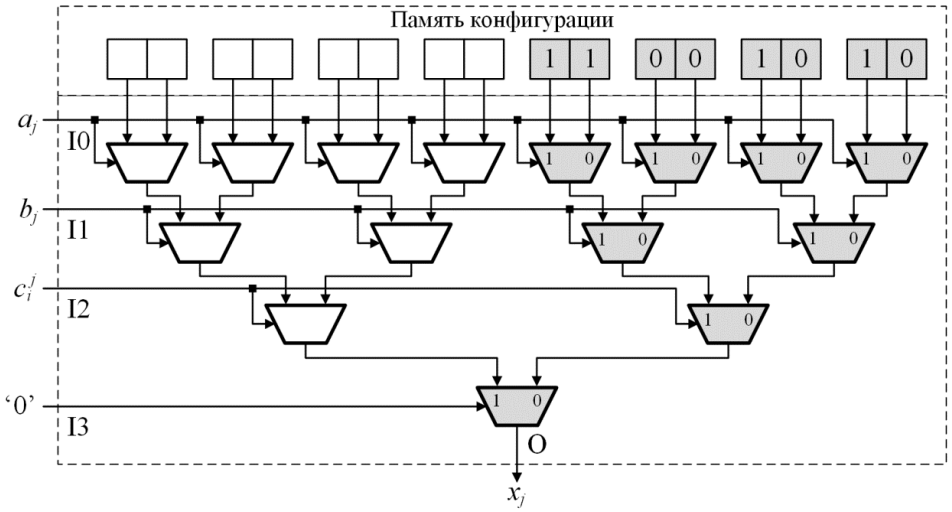


Рис. 3. Схемная реализация мультиплексора одного звена БСП ресурсами LUT-блока

Видно, что ресурс LUT-блока использован лишь наполовину. При больших значениях параметра *n* это может привести к существенным затратам на реализацию схемы А-ФНФ. Например, для $n=128$ реализация БСП для FPGA Spartan-3E будет использовать 256 LUT-блоков, которые составляют более 26 % от всех доступных ресурсов такого кристалла, как XC3S100E [12].

Предлагаемая архитектура симметричных путей. При реализации классической схемы БСП на FPGA каждый LUT-блок обладает уникальными параметрами, в том числе и временем срабатывания внутренних мультиплексоров, которые обеспечивают трансляцию выбранного сигнала на единственный выход.

Обозначим время распространения фронта тестового сигнала от входа a_j до выхода x_j как $\delta(x_j, a_j)$ для $c_i^j = 0$, а время распространения фронта тестового сигнала от входа b_j до выхода x_j как $\delta(x_j, b_j)$ для $c_i^j = 1$. Соответствующим образом введем обозначения для второго мультиплексора звена ЗВ_j: $\delta(y_j, a_j)$ для $c_i^j = 1$, $\delta(y_j, b_j)$ для $c_i^j = 0$. Для оценки перечисленных параметров воспользуемся параметрической моделью звена ЗВ_j, восстановленной после технологического синтеза для FPGA XC3S100E. Так, для звена ЗВ_0 параметры имеют следующие значения: $\delta(x_0, a_0) = 1{,}488$ нс, $\delta(x_0, b_0) = 1{,}445$ нс, $\delta(y_0, a_0) = 1{,}397$ нс, $\delta(y_0, b_0) = 1{,}465$ нс. Для смежного звена ЗВ_1 данные параметры будут принимать уже другие значения: $\delta(x_0, a_0) = 0{,}963$ нс, $\delta(x_0, b_0) = 1{,}016$ нс, $\delta(y_0, a_0) = 0{,}986$ нс, $\delta(y_0, b_0) = 0{,}993$ нс. Связано это в первую очередь с уникальностью самих LUT-блоков и с асимметрией конфигурируемых связей, их

соединяющих. Уникальные значения приведенных параметров позволяют реализовать вторую копию звена на свободных ресурсах одного LUT-блока. При этом ранее не использованный вход (I3 на рис. 3) будет применен для выбора первой либо второй копии звена. На рис. 4 показана новая структура звена БСП и схемотехническая реализация его верхней части на двух LUT-блоках с четырьмя входами. Представленная схема обеспечивает четыре конфигурации соединения входов a_j, b_j с выходами x_j, y_j: два прямых соединения при $c_i^j = 0$, $c_i^{j+1} = 0$ и $c_i^j = 1$, $c_i^{j+1} = 1$ и два перекрестных соединения при $c_i^j = 1$, $c_i^{j+1} = 0$ и $c_i^j = 0$, $c_i^{j+1} = 1$.

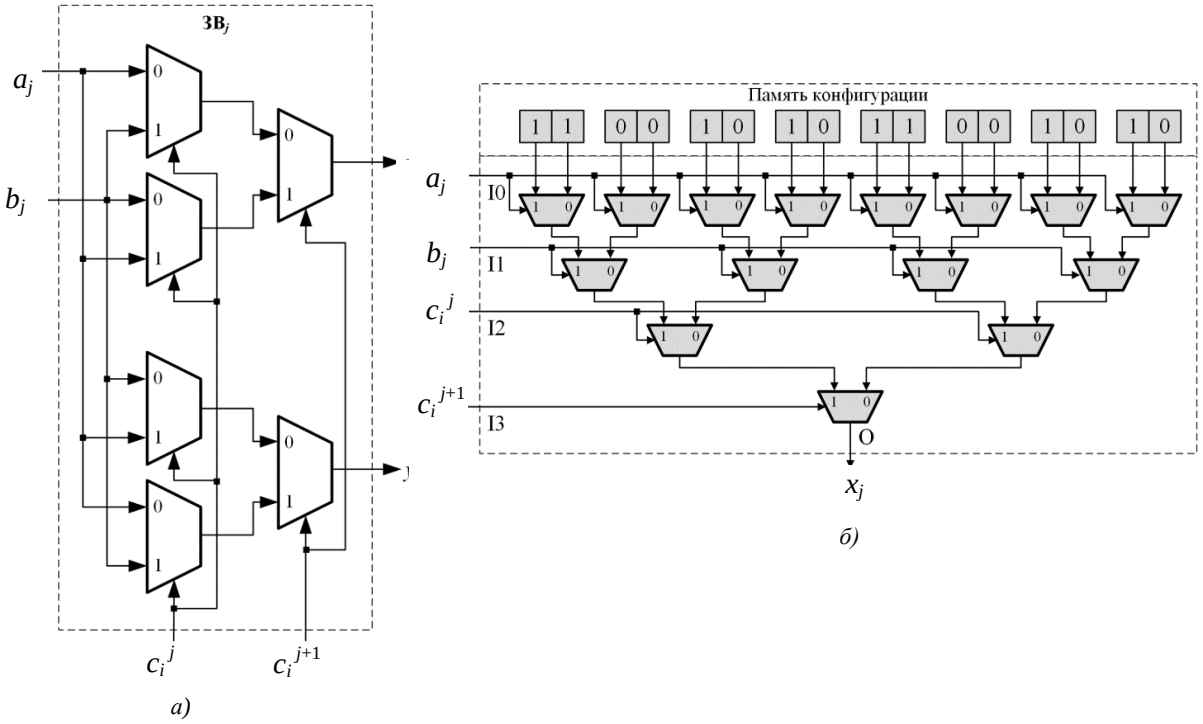


Рис. 4. Предлагаемая структура одного звена БСП (*а*) и схемная реализация его части на блоке LUT4 (*б*)

В табл. 1 представлены значения времени распространения фронта тестового сигнала от входов до выходов предложенной схемы в зависимости от значений c_i^j и c_i^{j+1} для двух различных звеньев одного БСП, полученные путем параметрического моделирования А-ФНФ с параметром $n = 16$ для FPGA SPARTAN-3E XC3S100E.

Таблица 1

Значения задержки распространения сигнала для двух различных звеньев БСП

Биты запроса, c_i^j c_i^{j+1}	Тип задержки	Значение задержки для звена ЗВ$_j$, нс	
		ЗВ$_2$	ЗВ$_1$
00	$\delta(x_j, a_j)$	0,950	1,394
	$\delta(y_j, b_j)$	0,861	0,992
01	$\delta(x_j, b_j)$	0,992	0,861
	$\delta(y_j, a_j)$	0,859	1,326
10	$\delta'(x_j, b_j)$	2,002	1,218
	$\delta'(y_j, a_j)$	0,191	1,168
11	$\delta'(x_j, a_j)$	0,060	1,037
	$\delta'(y_j, b_j)$	1,911	1,150

Представленные результаты свидетельствуют о потенциальной возможности использования предложенной архитектуры в качестве А-ФНФ.

Анализ аппаратных затрат. Как было показано ранее, предложенная структура звена БСП полностью вписывается в архитектуру блоков LUT4, что дает существенную экономию ресурсов FPGA-кристаллов. С учетом того что структурные блоки ГТС и АРБ (см. рис. 1) имеют незначительные затраты на реализацию (ГТС использует три LUT-блока и три триггера, АРБ использует один триггер в реализации, описанной в работе [5]), основная доля аппаратных затрат приходится на БСП. Предложенная архитектура звеньев БСП позволяет в два раза сократить аппаратные затраты в сравнении с классической архитектурой. В табл. 2 приведено сравнение аппаратных затрат при реализации двух схем А-ФНФ для FPGA XC3S100E.

Таблица 2

Аппаратные затраты на реализацию А-ФНФ ($n = 128$)

Название ресурса FPGA	Число использованных блоков		Число имеющихся блоков	Доля затрат, %	
	Классическая А-ФНФ	Предлагаемая А-ФНФ		Классическая А-ФНФ	Предлагаемая А-ФНФ
Slices	131	69	960	13,64	7,18
Flip-Flops	4	4	1920	0,141	0,141
4-input LUTs	259	131	1920	13,48	6,82

Из табл. 2 видно, что предлагаемая архитектура звеньев А-ФНФ позволяет почти в два раза сократить затраты на реализацию всей схемы и может быть реализована на FPGA с LUT-блоками, у которых число входов больше четырех [11].

Анализ основных характеристик ФНФ типа арбитр. Было проведено сравнение двух подходов к реализации А-ФНФ для FPGA XC3S100E с применением САПР Xilinx ISE 14.7 [13]. Для этого использовались две параметрические модели реализованных схем А-ФНФ с параметром $n=16$. В качестве схемы АРБ применялась схема синхронного D-триггера (технологический элемент FDC). Сами схемы А-ФНФ и тестовые модули к ним были описаны на языке Verilog. Тестовые модули, представляющие собой testbench-компоненты, осуществляли подачу всех возможных 2^n запросов на входы, генерирование тестового сигнала и анализ ответов схемы А-ФНФ. Кроме этого, тестовые модули осуществляли анализ временной разницы $\Delta(x_{n-1}, y_{n-1})$ между фронтами двух копий тестового сигнала, приходящих от выходов x_{n-1} и y_{n-1} на входы схемы АРБ.

На рис. 5 изображены три графика отсортированных по возрастанию значений временных различий, наблюдаемых на входах схемы АРБ, для трех различных реализаций: А-ФНФ-16 – классической схемы с числом звеньев $n=16$; А-ФНФ-16-Н и А-ФНФ-32-Н – схем с предложенной архитектурой звеньев $n=16$ и $n=32$ соответственно. При этом на оси абсцисс представлены не сами значения запросов, а их порядковые индексы C_{index}. Ввиду сложности генерирования всех возможных запросов для схемы А-ФНФ-32-Н, как и для остальных схем, были сгенерированы 2^{16} запросов. С целью обеспечения равномерности распределения этих запросов на множестве всех 2^{32} возможных значений использовался метод генерирования псевдослучайных М-последовательностей на основе 32-разрядной схемы LFSR. Отрицательные значения $\Delta(x_{n-1}, y_{n-1})$ на графиках означают, что фронт тестового сигнала с выхода y_{n-1} пришел позже, чем с выхода x_{n-1}.

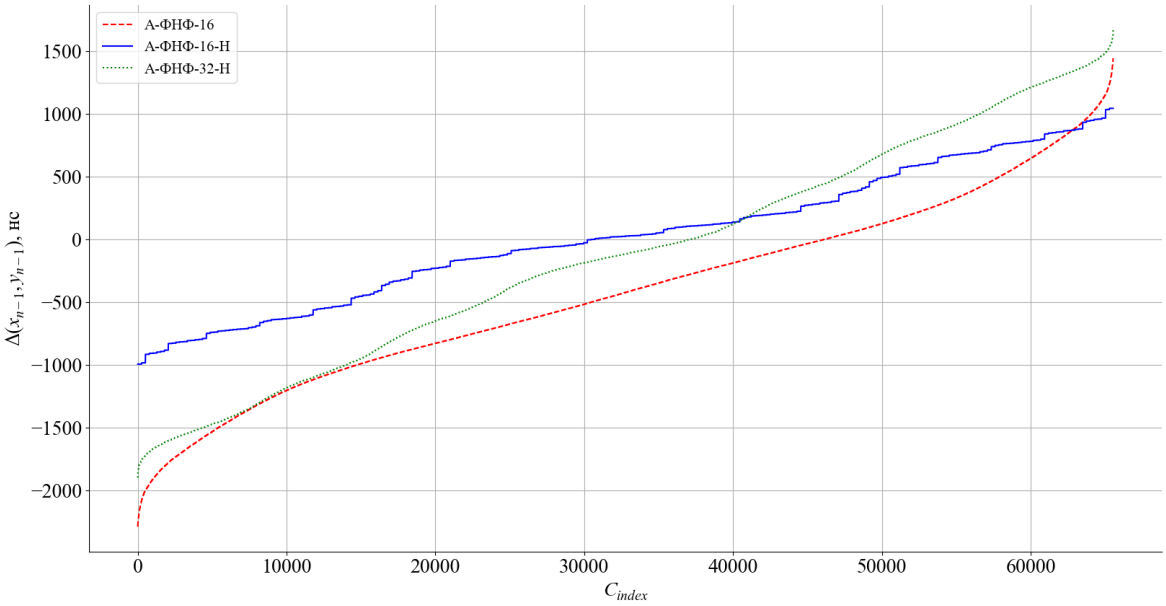
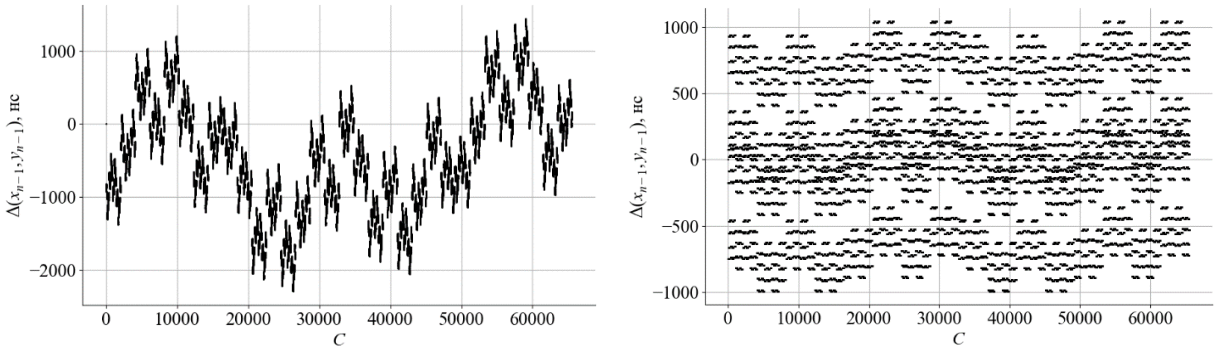


Рис. 5. Графики значений $\Delta(x_{n-1}, y_{n-1})$ для трех различных реализаций А-ФНФ

На рис. 5 видно, что графики значений $\Delta(x_{n-1}, y_{n-1})$ для А-ФНФ-16-Н и А-ФНФ-32-Н являются более симметричными относительно двух координатных осей, а их нелинейная форма усложняет зависимость между парами запрос-ответ в сравнении с классической схемой А-ФНФ-16. Асимметричность графика А-ФНФ-16 говорит о несбалансированности множества всех ответов, при которой вероятность появления нулевого ответа будет гораздо больше вероятности появления единичного ответа. Кроме этого, уменьшился диапазон результирующего значения $\Delta(x_{n-1}, y_{n-1})$. Так, для классической схемы А-ФНФ-16 этот диапазон равен [–2289; 1442] нс, а для предложенной архитектуры при том же параметре n он уменьшился и составляет [–994; 1043] нс. Обусловлено это в первую очередь фактическим уменьшением длин симметричных путей (числа LUT-блоков), что подтверждается оцененным диапазоном для схемы А-ФНФ-32-Н, равным [–1898; 1668] нс. Для каждой схемы также было оценено число ответов, при которых схема АРБ переходит в метастабильное состояние. Так, для схемы А-ФНФ-16 был получен 1241 метастабильный ответ, что составляет 1,89 % от всех зарегистрированных ответов. В то же время для схем А-ФНФ-16-Н и А-ФНФ-32-Н это значение равно 1,01 и 0,39 % соответственно, что является потенциальным показателем большей стабильности. Кроме того, в ходе экспериментов был оценен показатель внутрикристальной уникальности схем А-ФНФ-16 и А-ФНФ-16-Н путем реализации восьми идентичных компонентов на одном кристалле и сравнения множеств ответов при подаче одного множества различных запросов. Под внутрикристальной уникальностью понимается численный показатель, методика вычисления которого представлена в работе [6]. Этот показатель принимает значения в диапазоне [0;1] и характеризует степень различия множества ответов от реализованного на одном кристалле множества идентичных схем А-ФНФ при подаче на них одинаковых запросов. Значение уникальности, равное 0, означает, что все ответы являются идентичными. Значение показателя, равное 1, говорит о том, что все ответы от тестируемых схем А-ФНФ являются уникальными.

В итоге для схемы А-ФНФ-16 данный показатель уникальности равен 0,489, а для схемы А-ФНФ-16-Н равен 0,473, что свидетельствует о потенциальном применении данных схем для реализации уникальных неклонируемых идентификаторов. Реальные показатели стабильности и уникальности сильно зависят от параметра n, от схемы блока АРБ и могут быть оценены только на реальной аппаратуре [10] при многократной подаче одних и тех же запросов.

На рис. 6 показаны графики функциональной зависимости значений $\Delta(x_{n-1}, y_{n-1})$ от значений запросов, линейно упорядоченных по значению C от 0 до 65 535, для схем А-ФНФ-16 и А-ФНФ-16-Н.



а) *б)*

Рис. 6. Графики функциональной зависимости значений $\Delta(x_{n-1}, y_{n-1})$ от значений запросов:
а) для схемы А-ФНФ-16; *б)* для схемы А-ФНФ-16-Н

Как видно из представленных графиков, схема А-ФНФ-16-Н обладает большей случайностью и меньшей корреляционной зависимостью значений $\Delta(x_{n-1}, y_{n-1})$ от значений запросов C, что потенциально может усложнить построение точной математической модели схемы А-ФНФ злоумышленниками [4].

Заключение. В статье предложена новая архитектура звеньев блока симметричных путей для схемотехнической реализации физически неклонируемой функции типа арбитр на программируемых логических интегральных схемах типа FPGA. Показано, что за счет конфигурации встроенных LUT-блоков можно практически в два раза снизить аппаратные затраты на реализацию и при этом значительно улучшить качественные характеристики реализуемой ФНФ. Результаты описанных в статье экспериментов были получены с применением САПР Xilinx ISE 14.7 [13] и языка проектирования цифровой аппаратуры Verilog. Полученные результаты нуждаются в верификации на реальной аппаратуре с целью установления истинных показателей межкристальной уникальности, случайности, стабильности и возможности построения математической модели А-ФНФ методами машинного обучения. Предложенная схемная реализация также может быть применена для проектирования конфигурируемых ФНФ.

Список использованных источников

1. Design and implementation of high-quality physical unclonable functions for hardware-oriented cryptography / S. S. Zalivaka [et al.] // Secure System Design and Trustable Computing. – Switzerland : Springer, 2016. – P. 39–81.

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

3. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем / А. А. Иванюк. – Минск : Бестпринт, 2012. – 337 с.

4. Zalivaka, S. S. Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response / S. S. Zalivaka, A. A. Ivaniuk, Ch.-H. Chang // IEEE Transactions on Information Forensics and Security. – 2018. – Vol. 4, no. 14. – P. 1109–1123.

5. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation / S. S. Zalivaka [et al.] // Proc. IEEE/ACM Asia and South Pacific Design Automation Conf. – Macau, 2016. – P. 533–538.

6. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs / Y. Hori [et al.] // Proc. Intern. Conf. "Reconfigurable Computing and FPGAs". – Mexico, 2010. – P. 298–303.

7. Becker, G. T. On the pitfalls of using Arbiter-PUFs as building blocks / G. T. Becker // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. – 2015. – Vol. 34, no. 8. – P. 1295–1307.

8. A technique to build a secret key in integrated circuits for identification and authentication applications / J. W. Lee [et al.] // Proc. of the IEEE VLSI Circuits Symp. (VLSI'04). – Honolulu, 2004. – P. 176–179.

9. Morozov, S. An analysis of delay based PUF implementations on FPGA / S. Morozov, A. Maiti, P. Schaumont // Proc. Intern. Symp. "Applied Reconfigurable Computing". – Berlin, 2010. – P. 382–387.

10. Nexys 4 Artix-7 FPGA Trainer Board [Electronic resource]. – Mode of access: https:// store. digilentinc.com/nexys-4-artix-7-fpga-trainer-board-limited-time-see-nexys4-ddr. – Date of access: 20.11.2018.

11. 7 Series FPGAs Data Sheet: Overview [Electronic resource]. – Mode of access: https:// www.xilinx.com/ support/documentation/data_sheets/ds180_7Series_Overview.pdf. – Date of access: 20.11.2018.

12. Spartan-3E FPGA Family Data Sheety [Electronic resource]. – Mode of access: https:// www.xilinx.com/ support/documentation/data_sheets/ds312.pdf. – Date of access: 28.12.2018.

13. ISE Design Suite [Electronic resource]. – Mode of access: https://www.xilinx.com/products/ design-tools/ise-design-suite.html. – Date of access: 20.11.2018.

References

1. Zalivaka S. S., Zhang L., Klybik V. P., Ivaniuk A. A., Chang C.-H. Design and implementation of high-quality physical unclonable functions for hardware-oriented cryptography. *Secure System Design and Trustable Computing*. Switzerland, Springer, 2016, pp. 39–81. DOI: 10.1007/978-3-319-14971-4

2. Yarmolik V. N., Vashinko Y. G. Fizicheski nekloniruemye funkcii [Physically unclonable functions]. Informatika [*Informatics*], 2011, no. 2(30), pp. 92–103 (in Russian).

3. Ivaniuk A. A. Projektirovanie vstraivaemyh cifrovyh ustrojstv i system. *Design of Embedded Digital Devices and Systems*. Minsk, Bestprint, 2012, 337 p. (in Russian).

4. Zalivaka S. S., Ivaniuk A. A., Chang Ch.-H. Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response. *IEEE Transactions on Information Forensics and Security*, 2018, vol. 4, no. 14, pp. 1109–1123. DOI: 10.1109/TIFS.2018.2870835

5. Zalivaka S. S., Puchkov A. V., Klybik V. P., Ivaniuk A. A., Chang C.-H. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation. *Proceedings IEEE/ACM Asia and South Pacific Design Automation Conference*. Macau, 2016, pp. 533–538. DOI: 10.1109/ASPDAC.2016.7428066

6. Hori Y., Yoshida T., Katashita T., Satoh A. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs. *Proceedings International Conference "Reconfigurable Computing and FPGAs"*. Mexico, 2010, pp. 298–303. DOI: 10.1109/ReConFig.2010.24

7. Becker G. T. On the pitfalls of using Arbiter-PUFs as building blocks. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, vol. 34, no. 8, pp. 1295–1307. DOI: 10.1109/TCAD.2015.2427259

8. Lee J. W., Gassend B., Lim D., Suh G. E. A technique to build a secret key in integrated circuits for identification and authentication applications. *Proceedings of the IEEE VLSI Circuits Symposium (VLSI'04)*. Honolulu, 2004, pp. 176–179. DOI: 10.1109/VLSIC.2004.1346548

9. Morozov S., Maiti A., Schaumont P. An analysis of delay based PUF implementations on FPGA. *Proceedings International Symposium "Applied Reconfigurable Computing"*. Berlin, 2010, pp. 382–387. DOI: 10.1007/978-3-642-12133-3_37

10. Nexys 4 Artix-7 FPGA Trainer Board. Available at: https:// store.digilentinc.com/nexys-4-artix-7-fpga-trainer-board-limited-time-see-nexys4-ddr (accessed 20.11.2018).

11. 7 Series FPGAs Data Sheet: Overview. Available at: https:// www.xilinx.com/support/documentation/ data_sheets/ds180_7Series_Overview.pdf (accessed 20.11.2018).

12. Spartan-3E FPGA Family Data Sheety. Available at: https:// www.xilinx.com/support/documentation/ data_sheets/ds312.pdf (accessed 28.12.2018).

13. ISE Design Suite. Available at: https://www.xilinx.com/products/design-tools/ise-design-suite.html (accessed 20.11.2018).

Информация об авторе

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

Information about the author

Alexander A. Ivaniuk, Dr. Sci. (Eng.), Professor Computer Science Department, Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus.
E-mail: ivaniuk@bsuir.by