УДК 004.056.5

ФИЗИЧЕСКАЯ КРИПТОГРАФИЯ И ЗАЩИТА ЦИФРОВЫХ УСТРОЙСТВ

А.А. ИВАНЮК, С.С. ЗАЛИВАКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 11 февраля 2019

Аннотация. В статье представлены основные научные результаты и достижения, полученные аспирантами, магистрантами и соискателями кафедры информатики БГУИР под научным руководством профессора А.А. Иванюка в период с 2014 по 2018 год. Приведены оригинальные схемотехнические решения в области синтеза цифровых физически неклонируемых функций. Впервые проблематика физически неклонируемых функций была опубликована в 2011 году в журнале «Информатика» профессором кафедры ПОИТ БГУИР д.т.н., профессором В.Н. Ярмоликом, являющимся известным отечественным ученым в области проектирования надежных цифровых устройств и систем. В данной статье приведены новые методы и алгоритмы неклонируемой идентификации и аутентификации цифровых устройств. Представлены результаты, полученные в области генерирования случайных числовых последовательностей. Кроме того, приведены результаты по методам реализации аппаратных водяных знаков и функциональной обфускации цифровых устройств.

Ключевые слова: физически неклонируемые функции, цифровые устройства, программируемые логические интегральные схемы, идентификация, аутентификация, случайные числовые последовательности, аппаратные водяные знаки, функциональная обфускация.

Abstract. The article presents the main scientific results and practical achievements obtained by undergraduate and graduate students of Computer Science department of BSUIR under the supervision of professor A.A. Ivaniuk during the period from 2014 to 2018. The original circuit solutions in the field of synthesis of digital physically unclonable functions are presented. The area of physically unclonable functions was first time published in the journal «Informatics» by professor of Software for information technologies department of BSUIR, doctor of technical sciences V.N. Yarmolik, which is a famous domestic scientist in area of reliable digital devices and systems design. New methods and algorithms for unclonable identification and authentication of digital devices are described. The paper also presents the results obtained in the field of random number sequences generation. In addition, the results on the methods of hardware watermarks injection and functional obfuscation of digital devices are given.

Keywords: physically unclonable functions, digital devices, field programmable gate arrays, identification, authentication, random number sequences, hardware watermarks, functional obfuscation.

Doklady BGUIR. 2019, Vol. 120, No. 2, pp. 50-58
Physical cryptography and security of digital devices
A.A. Ivaniuk, S.S. Zalivaka

Введение

Количество устройств Интернета вещей (IoT), соединенных между собой, к 2020 году достигнет порядка 50 млрд. В то же время, количество криптографических атак на данный класс устройств также возрастает. В связи с этим актуальной научной и практической задачей является разработка аппаратных методов и средств защиты цифровых устройств от нелегального доступа, копирования, модификации и обратного проектирования. В настоящее время данный класс задач может быть эффективно решен с помощью методов физической криптографии. В статье кратко приводятся основные научные и технические

результаты, полученные в области исследования физически неклонируемых функций (ФНФ) для решения задач генерирования случайных числовых последовательностей, идентификации и аутентификации. Поскольку реализации ФНФ являются компактными и высокопроизводительными, они подходят для решения задач аппаратной безопасности устройств IoT. Помимо этого, приводятся результаты по внедрению аппаратных цифровых водяных знаков и функциональной обфускации, которые также актуальны для защиты цифровых устройств и их проектных описаний.

Генерирование случайных числовых последовательностей

Особенностью ФНФ, реализованных на кристалле интегральной схемы, является их двойственная природа. С одной стороны, пары запрос-ответ ФНФ представляют собой уникальную характеристику устройства и тем самым могут быть использованы в качестве идентификатора. В то же время непустое подмножество пар запрос-ответ является нестабильным. Следовательно, ФНФ могут быть использованы для реализации генераторов случайных числовых последовательностей (ГСЧП). В отличие от генераторов псевдослучайных числовых последовательностей (ГПСЧП), основанных на физических реализациях математических моделей и алгоритмов, генераторы на основе ФНФ действительно случайны, что позволяет использовать их в аппаратных реализациях криптографических алгоритмов, например, в качестве генераторов секретных ключей.

В настоящее время существует два основных подхода к реализации ГСЧП, источником случайности которых является ФНФ [1]. Первый подход заключается в использовании ГПСЧП с периодически изменяемым случайным начальным состоянием, вырабатываемым ФНФ. Недостатком данного подхода являются дополнительные аппаратурные затраты, требующиеся на реализацию ГПСЧП. Второй подход, в свою очередь, использует выходные значения ответов ФНФ, отбирая те из них, случайность которых максимальна. Одним из критериев случайности является соотношение нулей и единиц в формируемой последовательности ответов. Достоинством второго подхода являются небольшие аппаратурные затраты, поскольку требуется реализовать только ФНФ. Недостатком является потеря производительности, необходимая для выбора подмножества пар запрос-ответ из экспоненциально большого множества, а также для непосредственного генерирования последовательности.

В работе [2] авторами был предложен ГСЧП на основе модицифированной ФНФ кольцевых генераторов. Генератор реализован на основе первого подхода, т. е. в качестве ГПСЧП были использованы дерево элементов XOR и одноканальный сигнатурный анализатор. Спроектированный генератор является реконфигурируемым, и его настройка осуществляется по четырем параметрам: длительность одиночного импульса X, количество элементов ФНФ кольцевых генераторов K, количество инверторов N в каждом блоке ФНФ, а также разрядность одноканального сигнатурного анализатора D. Генератор был реализован на ПЛИС Xilinx Spartan 3E-500 и по аппаратурным затратам является более эффективным по сравнению с существующими решениями на основе ФНФ кольцевых генераторов.

ГСЧП на основе эмуляции элементов статического оперативного запоминающего устройства (ОЗУ) был предложен авторами в работе [3]. Данный генератор реализован на основе первого подхода, поскольку использует адаптивный сигнатурный анализатор, применяемый для приведения вырабатываемой последовательности к равномерному статистическому распределению. Предложенная модификация ФНФ на основе эмуляции статического ОЗУ позволяет решить не только задачу генерирования случайных числовых последовательностей, но и идентификации. Кроме того, для ее реализации требуется как минимум в 4 раза меньше аппаратуры в сравнении с ФНФ на основе кольцевых генераторов [2]. Недостатком ГСЧП является необходимость асинхронного сброса для генерирования следующего случайного числа, что снижает производительность.

В работе [1] был сформулирован метод структурного синтеза ГСЧП на основе ФНФ, который является обобщением работ [2, 3]. Предложенный метод был рассмотрен на примере реализации трех различных ГСЧП: на основе ФНФ кольцевых генераторов, дерева XOR и одноканального сигнатурного анализатора; ФНФ на основе эмуляции СОЗУ и адаптивного сигнатурного анализатора; ФНФ типа арбитр и многоканального сигнатурного анализатора.

Авторами было показано, что использование ФНФ в качестве источника случайности позволяет проектировать ГСЧП с различной производительностью, аппаратурными затратами и статистическими свойствами вырабатываемой последовательности. При этом характеристики генератора зависят только от выбора типа ФНФ и схемы ГПСЧП.

В работах [4–5] множество пар запрос-ответ ФНФ типа арбитр было разделено на подмножество стабильных и нестабильных. Ответы, соответствующие нестабильным парам, были использованы для генерирования случайной числовой последовательности. Разработанный алгоритм соответствует второму подходу к проектированию ГСЧП на основе ФНФ, поэтому не требует дополнительных аппаратурных затрат, однако ухудшает скорость выработки случайной последовательности.

Разработанные авторами ГСЧП были проверены на соответствие стандарту NIST для действительно случайных числовых последовательностей. Было показано, что использование ФНФ в качестве источника случайности позволяет сократить аппаратурные затраты, а также улучшить качество вырабатываемых случайных последовательностей по сравнению с существующими решениями.

Неклонируемая идентификация и аутентификация

Для разработки методов неклонируемой идентификации и аутентификации авторами была выбрана ФНФ типа арбитр (А-ФНФ) по причинам приемлемых аппаратурных затрат, экспоненциально большой мощности множества пар запрос-ответ, а также высоких значений характеристик случайности и уникальности по сравнению с другими классическими реализациями ФНФ на ПЛИС типа FPGA (ФНФ кольцевых генераторов, ФНФ на основе памяти и ФНФ на основе бистабильных элементов).

Одной из главных проблем при использовании ФНФ в качестве генератора уникальных идентификаторов, а также при реализации протоколов аутентификации является наличие нестабильного подмножества пар запрос-ответ. Существует два основных класса подходов к решению данной проблемы: корректировка ответов и схемотехническое изменение ФНФ. Недостатком первого класса методов являются значительные аппаратурные и временные затраты на реализацию кодов коррекции ошибок, если базовая стабильность ФНФ была невысокой. Второй класс подходов более специфичен к конкретным архитектурам ФНФ и, как правило, технически более сложен. К сожалению, существующие реализации классической архитектуры А-ФНФ обладают низкой стабильностью в силу перехода схемы арбитра в метастабильное состояние.

В работе [5] были предложены две схемотехнические модификации схемы арбитра: на основе четырех синхронных D-триггеров и на основе асинхронного RS-триггера. Первая модификация позволяет рассматривать не только передний фронт тестового сигнала для генерирования ответа А-ФНФ, а весь импульс в целом. Таким образом, предложенная схема позволяет обнаруживать разную длительность двух копий тестового сигнала, а также с большей вероятностью определять малые различия во времени прихода фронтов и спадов рассматриваемых сигналов. В основу второй модификации положено явление затухающего колебания асинхронного RS-триггера при попытке сохранить запрещенное состояние. Как было показано авторами, при небольших различиях во времени прихода спада тестового сигнала RS-триггер на выходе производит высокочастотное затухающее колебание, наличие которого свидетельствует о переходе триггера в метастабильное состояние. Предложенные схемотехнические модификации позволили значительно улучшить характеристику стабильности А-ФНФ при реализации на FPGA с 0,57 до 0,99 с учетом дополнительных аппаратурных затрат, не превышающих 2 % от исходной реализации схемы арбитра. Для детального исследования особенностей схемных реализаций А-ФНФ в работе [7] была предложена мультиарбитральная схема, в которой арбитр помещается после каждого звена симметричных путей. Моделирование и реализация предложенной схемы показали зависимость такой характеристики, как стабильность, от длины симметричных путей. Было подтверждено, что, несмотря на переход арбитра в состояние метастабильности, возможно применение мультиарбитральной ФНФ для уникальной идентификации цифровых устройств. Кроме этого, экспериментально было продемонстрировано, что зависимость пар запрос-ответ имеет линейную природу.

В работах [4, 6, 8] была разработана математическая модель А-ФНФ, особенностью которой является описание метастабильного состояния арбитра. Предложенная модель позволяет улучшить характеристику стабильности А-ФНФ до 1,0 в условиях изменения температуры окружающей среды от –40 до 90° С без дополнительных аппаратурных затрат. Модель описывает разности задержек распространения сигналов в виде линейной функции, которая зависит от бинарных значений запроса, а также уникальных характеристик каждого из звеньев А-ФНФ. На основе модели был разработан алгоритм классификации запросов, позволяющий разделить множество пар запрос-ответ на сильные, характеристика стабильности которых с высокой вероятностью (0,99) имеет высокое значение, и слабые, значения ответа для которых нестабильны. Предложенный алгоритм позволяет генерировать неклонируемые идентификаторы с высоким значением характеристик уникальности (0,511) и стабильности (1,0). В свою очередь, на основе слабых пар запрос-ответ возможно построение ГСЧП.

Авторами было показано, что характеристики стабильности и случайности А-ФНФ являются обратно пропорциональными, т. е. улучшение одной из них ведет к ухудшению другой. Следовательно, модификации А-ФНФ с повышенной стабильностью ответов становятся уязвимы к моделированию с помощью методов машинного обучения. В свою очередь, данная уязвимость позволяет злоумышленнику осуществить криптографические атаки на протоколы безопасности, реализованные на основе А-ФНФ.

В работах [6, 9] были предложены модификации А-ФНФ с помощью регистра из Т-триггеров, а также многоканального сигнатурного анализатора MISR. Данный подход позволяет преобразовать линейную зависимость между значением запроса и ответа А-ФНФ в нелинейную, тем самым значительно усложняя задачу злоумышленника по осуществлению криптографической атаки. Таким образом, уязвимость А-ФНФ к классическим атакам с помощью метода опорных векторов и логистической регрессии была снижена с 98 до 50 %. Несмотря на это, предложенные модификации подвергаются криптографической атаке методом эволюционной стратегии адаптации ковариационных матриц, который в настоящее время является стандартом атак на ФНФ.

В работе [8] был предложен протокол аутентификации на основе А-ФНФ, который является практически стойким к атаке с помощью эволюционной стратегии. Вместо хранения экспоненциально большого множества пар запрос-ответ была предложена точная программная модель А-ФНФ, построенная на основе 5 классов пар запрос-ответ и 20-слойной искусственной нейронной сети. Для нелинейного преобразования запросов также был использован многоканальный сигнатурный анализатор. Эксперименты показали, что криптографическая атака может быть осуществлена, однако на ее осуществление потребуется более 100 лет работы многопроцессорного сервера.

Полученные в работах [4–6, 8–12] результаты показали, что реализация А-ФНФ на ПЛИС типа FPGA может быть использована для надежной неклонируемой идентификации цифровых устройств, реализации протоколов аутентификации со сниженной уязвимостью к крипографическим атакам, а также генераторов случайных числовых последовательностей. Более того, все разработки, предложенные авторами, были экспериментально верифицированы с помощью реконфигурируемых аппаратно-программных комплексов, что позволяет сделать вывод о том, что предложенные решения могут быть также реализованы с помощью специализированных ИС.

В настоящее время проводятся исследования характеристик и особенностей функционирования интегральных схем динамических ОЗУ с целью построения на их основе уникальных неклонируемых идентификаторов [13]. Кроме того, осуществляется поиск технических решений применения ФНФ для обеспечения безопастности IoT на примере инфраструктуры цифровых устройств умного дома [12].

Цифровые водяные знаки и схемотехническая обфускация

Проектные описания цифровых устройств составляются при помощи специальных языков проектирования аппаратуры HDL (Hardware Description Language). Так, HDL применяется для составления высокоуровневого описания цифровой схемотехники проектируемого устройства на различных уровнях абстракции. Типичное HDL-описание

содержит в себе информацию как о структуре устройства, так и о функционале всего устройства либо его составных компонент. Преобразование из HDL-описания в схемное описание называется синтезом и включает в себя множество этапов, в том числе структурную и логическую оптимизацию. В совокупности с использованием последовательных и параллельных HDL-операторов известные методы защиты программного обеспечения не могут быть применены для проектных описаний цифровых устройств. Например, хорошо зарекомендовавшие себя методы запутывающих преобразований (обфускации), защищающие исходные коды программ от обратного проектирования, и методы постановки водяных знаков, защищающие авторские права разработчиков, теряют свой смысл при процедурах RTL (Register Transfer Level) и технологического синтеза. Таким образом, разработка подобных методов защиты цифровых устройств и их проектных описаний являются актуальными научно-техническими задачами.

В работе [14] было дано определение аппаратного водяного знака (АВЗ) и описаны его свойства. Так, под АВЗ следует понимать цифровый водяной знак, встраиваемый в проектное описание цифрового устройства с целью защиты авторских прав проектировщика как на само проектное описание, так и на готовое цифровое устройство. При этом АВЗ должен нести уникальную информацию о проектировщике (и/или защищаемом устройстве), а процедура использования АВЗ содержит два этапа: встраивание и извлечение АВЗ. Было показано, что АВЗ должны удовлетворять следующему свойству: $DD(V) = SCH$; $DD(V^*) = SCH^*$; $FUNC(SCH) = FUNC(SCH^*)$, где V – проектное HDL-описание, V^* – описание, содержащее авторский водяной знак, DD – процедура синтеза, SCH – результирующее схемное представление устройства, SCH^* – схемное представление, содержащее водяной знак, $FUNC$ – функциональная спецификация устройства.

Процедура WM постановки АВЗ при этом формально описывается как $V^* = WM(V,K)$, где K – сообщение, однозначно идентифицирующее автора. В свою очередь, процедура EX извлечения АВЗ должна определять присутствие или отсутствие сообщения K в исходном описании V^* и/или синтезированной схеме SCH^*: $EX(V^*,K) = EX(SCH^*,K) = true$.

Процедура внедрения АВЗ не должна нарушать функциональную корректность проектного описания. Кроме того, АВЗ должен обладать следующими основными характеристиками [14]: стойкость, емкость, затраты на встраивание (извлечение), вносимые издержки, скрытность, прозрачность. На основе определенных характеристик АВЗ была создана их классификация [14] по назначению (идентификация автора, доказательство подлинности либо доказательство передачи), по уровням (одноуровневые и многоуровневые), по устойчивости к изменениям (устойчивые и хрупкие), по процессу построения (статические и динамические), по обнаруживаемости (детерминированные и вероятностные), по источникам извлечения (сторонние каналы, порты, бит-образы ПЛИС и др.). Было показано, что наиболее перспективными для реализации являются динамические многоуровневые АВЗ, внедряемые на различных уровнях абстракции проектных описаний, обладающие необходимыми перечисленными характеристиками. Так, динамические АВЗ обладают большей скрытностью в сравнении со статическими знаками, а наличие многоуровневых АВЗ позволяет им быть прозрачными для средств синтеза и оптимизации.

Для улучшения характеристики скрытности АВЗ дополнительно применяют запутывающие преобразования, именуемые обфускацией. В работах [15–17] было показано, что в большинстве случаев применение методов лексической обфускации для проектных описаний является неприемлемым ввиду трансляции высокоуровневых языковых HDL-конструкций различных уровней абстракции к схемотехническому представлению устройства. В работе [18] был предложен новый вид запутывающих преобразований, названный функциональной обфускацией, под которой понимается процесс применения запутывающих преобразований к цифровой схеме устройства SCH с целью получения более сложной для понимания схемы SCH^*, имеющей эквивалентную функциональность. Было показано, что методы функциональной обфускации должны обладать схожими характеристиками с АВЗ, и, в первую очередь, они должны быть прозрачными для средств синтеза и оптимизации.

Помимо функциональной обфускации применение лексической обфускации также важно для защиты проектных описаний от атак обратного проектирования. В свою очередь,

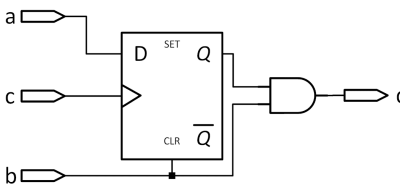
недостатком функциональной обфускации является увеличение аппаратной сложности и ухудшение временных характеристик устройства. Применение обоих типов обфускации обеспечивает высокий уровень защиты на всех стадиях жизненного цикла устройства.

Для оценки качества лексической обфускации в работе [18] была предложена новая метрика сложности проектных описаний с учетом особенностей языка проектирования VHDL: $C(V)=\sum_{i=0}^{8}(a_i * M_i)$, где a_i – весовой коэффициент, выбранный для метрики, M_i – рассчитанное значение i-й метрики проектного описания V. На многих отобранных примерах реальных проектных описаний было показано, что следующие перечисленные метрики являются значимыми для оценки общей сложности: M_1 – число операторов; M_2 – среднее число операторов в параллельном выражении; M_3 – число параллельных выражений; M_4 – число сигналов и переменных; M_5 – сцепление параллельных операторов; M_6 – средний размер списка чувствительных сигналов параллельных процессов; M_7 – число деклараций (типов, сигналов, переменных и т. д.); M_8 – метрика пространственной сложности. При верификации значений $C(V)$ было показано, что минимальные значения, вероятнее всего, свидетельствуют о хорошем качестве и стиле исходного VHDL-кода.

В области функциональной обфускации в работах [15, 17] были предложены схемотехнические решения построения так называемых генераторов константных значений CVG (Constant Value Generator), представляющие собой смешанные схемы, поведение которых описывается как переключательной, так и последовательностной логикой. Данное свойство позволяет схемам CVG быть прозрачными для средств синтеза, а вырабатываемые ими константные значения могут быть применены как для функциональной обфускации других цифровых компонент, так и для построения аппаратных водяных знаков (рисунок).

```
process( a, b, c ) begin
       if( b='1' ) then
              s <= '0';
       elsif ( rising_edge( c ) )  then
              s <= a;
       end if;
end process;
q <= s and b;
```

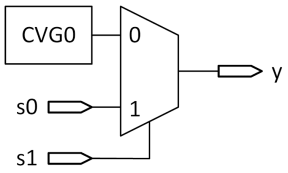
а



б

```
process(O1o0l10i,0lo0110i,olo01101)begi
n if(Olo0110i='1') then olo0ll01<='0';
elsif(rising_edge(olo01101)) then
olo0ll01<=O1o0l10i; end if; end
process; o100ll01<=olo0ll01 and
Olo0110i;
```

в



г

Пример CVG: *а* – исходное VHDL-описание; *б* – результат лексической обфускации; *в* – результат синтеза CVG; *г* – применение CVG для функциональной обфускации

Результаты, полученные в области аппаратных водяных знаков и функциональной обфускации, были апробированы и доказали свою состоятельность для САПР программируемых логических интегральных схем, языков проектирования VHDL и Verilog.

Заключение

Научная группа под руководством А.А. Иванюка продолжает активно проводить исследования методов идентификации, аутентификации и генерирования случайных числовых последовательностей на основе физически неклонируемых функций, реализуемых как на программируемых логических интегральных схемах, так и на запоминающих устройствах, в том числе на устройствах энергонезависимой флеш-памяти. Ведутся поиски новых схемотехнических решений ФНФ типа арбитр, конфигурируемых ФНФ и цифровых схем, позволяющих одновременно решать задачу неклонируемой идентификации и генерирования СЧП.

Полученные научные результаты докладывались как на отечественных, так и на международных конференциях и симпозиумах, среди которых необходимо отметить

следующие: IEEE Asia and South Pacific Design Automation Conference, International Conference on Digital Technologies, IEEE International Symposium on Quality Electronic Design, IEEE International Symposium on Circuits & Systems, Информационные технологии и системы.

Экспериментальные исследования схемотехнических реализаций ФНФ при различных условиях окружающей среды с помощью температурной камеры, а также моделирование криптографических атак на ФНФ типа арбитр с помощью высокопроизводительных вычислительных серверов были проведены совместно с Наньянгским технологическим университетом (Сингапур).

Некоторые научные результаты были включены в монографию «Secure System Design and Trustable Computing», выпущенную в 2016 году издательством Springer. В 2018 году результат, полученный в области надежной неклонируемой аутентификации цифровых устройств, был опубликован в престижном международном журнале «IEEE Transactions on Information Forensics and Security». В период с 2014 по 2018 год по представленным научным направлениям было защищено 10 дипломных проектов, восемь магистерских и одна кандидатская диссертация.

Список литературы

1. Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography. Secure System Design and Trustable Computing / S.S. Zalivaka [et al.]. Switzerland: Springer, 2016. Ch. 2. P. 39–81.
2. Заливако С.С., Иванюк А.А. Использование физически неклонируемых функций для генерирования действительно случайных числовых последовательностей // Автоматика и вычислительная техника. 2013. № 3. С. 61–72.
3. Заливако С.С., Иванюк А.А. Схемная реализация комбинированной физически неклонируемой функции для генерирования действительно случайных числовых последовательностей // Докл. БГУИР. 2013. № 7 (77). С. 37–43.
4. Заливако С.С., Иванюк А.А., Клыбик В.П. Метод увеличение стабильности физически неклонируемой функции типа «арбитр» // Информатика. 2017. № 1 (53). С. 31–43.
5. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation / S.S. Zalivaka [et al.] // Invited Paper at Special Session on Cyber-Physical Systems and Security, in Proc. 21st IEEE Asia and South Pacific Design Automation Conf. (ASP-DAC 2016). Macao, China, 26–28 January 2016. P. 533–538.
6. Zalivaka S.S., Ivaniuk A.A., Chang C.H. FPGA Implementation of Modeling Attack Resistant Arbiter PUF with Enhanced Reliability // Invited Paper at Special Session on IoT Security: Protocol, Implementation and Attacks, in Proc. 18st IEEE International Symposium on Quality Electronic Design (ISQED 2017). Santa Clara, CA, USA, 13–15 March 2017. P. 313–318.
7. Klybik V.P., Ivaniuk A.A. Use of arbiter physical unclonable function to solve identification problem of digital devices // Automatic Control and Computer Sciences. 2015. Vol. 49, № 3. P. 139–147.
8. 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. № 4 (14). P. 1109–1123.
9. Zalivaka S.S., Ivaniuk A.A., Chang C.H. Low-cost Fortification of Arbiter PUF Against Modeling Attack // Proc. of IEEE International Symposium on Circuits & Systems (ISCAS 2017). Baltimore, MD, USA, 28–31 May 2017. P. 1600–1603.
10. Заливако С.С., Иванюк А.А. Обзор методов активной идентификации цифровых устройств // Информатика. 2016. № 3 (51). С. 38–48.
11. Иванюк А.А. Особенности реализации симметричных путей ФНФ типа арбитр на ПЛИС // Матер. междунар. науч. конф. «Информационные технологии и системы 2018». Минск, 25 октября 2018 г. С. 156–157.
12. Клыбик В.П., Иванюк А.А. Перспективные возможности обеспечения безопасности инфраструктуры IoT // Матер. междунар. науч. конф. «Информационные технологии и системы 2018». Минск, 25 октября 2018 г. С. 162–163.
13. Пучков А.В., Иванюк А.А. Применение запоминающих устройств в качестве криптографических примитивов для интегральных схем программируемой логики // Материалы междунар. науч. конф. «Информационные технологии и системы 2016». Минск, 26 октября 2016 г. С. 210–211.
14. Сергейчик В.В., Иванюк А.А. Обзор методов реализации аппаратных водяных знаков в цифровых устройствах программируемой логики // Информатика. 2015. № 1 (45). С. 102–112.

15. Sergeichik V.V., Ivaniuk A.A. Implementation of opaque predicates for FPGA designs hardware obfuscation // J. of Information, Control and Management Systems. 2014. № 12 (2). P. 177–188.
16. Sergeichik V.V., Ivaniuk A.A. Digital Watermark and Fingerprint in Variable Rank Linear-Feedback Shift Register // Automatic Control and Computer Sciences. 2016. Vol. 50, № 2. P. 107–115.
17. Sergeichik V., Ivaniuk A. Hardware Primitives for FPGA Design Obfuscation // Proceedings of the Section of Young Researchers and Scientists (SYRAS) on the 10th International Conference on Digital Technologies 2014. Zilina, Slovakia, 9–11 July 2014. P. 39–44.
18. Сергейчик В.В., Иванюк А.А. Особенности обфускации VHDL-описаний и методы оценки ее сложности // Информатика. 2014. № 1 (41). С. 116–125.

References

1. Design and Implementation of High-Quality Physical Unclonable Functions for Hardware-Oriented Cryptography. Secure System Design and Trustable Computing / S.S. Zalivaka [et al.]. Switzerland: Springer, 2016. Ch. 2. P. 39–81.
2. Zalivako S.S., Ivanjuk A.A. Ispol'zovanie fizicheski nekloniruemyh funkcij dlja generirovanija dejstvitel'no sluchajnyh chislovyh posledovatel'nostej // Avtomatika i vychislitel'naja tehnika. 2013. № 3. S. 61–72. (in Russ.)
3. Zalivako S.S., Ivanjuk A.A. Shemnaja realizacija kombinirovannoj fizicheski nekloniruemoj funkcii dlja generirovanija dejstvitel'no sluchajnyh chislovyh posledovatel'nostej // Dokl. BGUIR. 2013. № 7 (77). S. 37–43. (in Russ.)
4. Zalivako S.S., Ivanjuk A.A., Klybik V.P. Metod uvelichenie stabil'nosti fizicheski nekloniruemoj funkcii tipa «arbitr» // Informatika. 2017. № 1 (53). S. 31–43. (in Russ.)
5. Multi-valued arbiters for quality enhancement of PUF responses on FPGA implementation / S.S. Zalivaka [et al.] // Invited Paper at Special Session on Cyber-Physical Systems and Security, in Proc. 21st IEEE Asia and South Pacific Design Automation Conf. (ASP-DAC 2016). Macao, China, 26–28 January 2016. P. 533–538.
6. Zalivaka S.S., Ivaniuk A.A., Chang C.H. FPGA Implementation of Modeling Attack Resistant Arbiter PUF with Enhanced Reliability // Invited Paper at Special Session on IoT Security: Protocol, Implementation and Attacks, in Proc. 18st IEEE International Symposium on Quality Electronic Design (ISQED 2017). Santa Clara, CA, USA, 13–15 March 2017. P. 313–318.
7. Klybik V.P., Ivaniuk A.A. Use of arbiter physical unclonable function to solve identification problem of digital devices // Automatic Control and Computer Sciences. 2015. Vol. 49, № 3. P. 139–147.
8. 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. № 4 (14). P. 1109–1123.
9. Zalivaka S.S., Ivaniuk A.A., Chang C.H. Low-cost Fortification of Arbiter PUF Against Modeling Attack // Proc. of IEEE International Symposium on Circuits & Systems (ISCAS 2017). Baltimore, MD, USA, 28–31 May 2017. P. 1600–1603.
10. Zalivako S.S., Ivanjuk A.A. Obzor metodov aktivnoj identifikacii cifrovyh ustrojstv // Informatika. 2016. № 3 (51). S. 38–48. (in Russ.)
11. Ivanjuk A.A. Osobennosti realizacii simmetrichnyh putej FNF tipa arbitr na PLIS // Mater. mezhdunar. nauch. konf. «Informacionnye tehnologii i sistemy 2018». Minsk, 25 oktjabrja 2018 g. S. 156–157. (in Russ.)
12. Klybik V.P., Ivanjuk A.A. Perspektivnye vozmozhnosti obespechenija bezopasnosti infrastruktury IoT // Mater. mezhdunar. nauch. konf. «Informacionnye tehnologii i sistemy 2018». Minsk, 25 oktjabrja 2018 g. S. 162–163. (in Russ.)
13. Puchkov A.V., Ivanjuk A.A. Primenenie zapominajushhih ustrojstv v kachestve kriptograficheskih primitivov dlja integral'nyh shem programmiruemoj logiki // Materialy mezhdunar. nauch. konf. «Informacionnye tehnologii i sistemy 2016». Minsk, 26 oktjabrja 2016 g. S. 210–211. (in Russ.)
14. Sergejchik V.V., Ivanjuk A.A. Obzor metodov realizacii apparatnyh vodjanyh znakov v cifrovyh ustrojstvah programmiruemoj logiki // Informatika. 2015. № 1 (45). S. 102–112. (in Russ.)
15. Sergeichik V.V., Ivaniuk A.A. Implementation of opaque predicates for FPGA designs hardware obfuscation // J. of Information, Control and Management Systems. 2014. № 12 (2). P. 177–188.
16. Sergeichik V.V., Ivaniuk A.A. Digital Watermark and Fingerprint in Variable Rank Linear-Feedback Shift Register // Automatic Control and Computer Sciences. 2016. Vol. 50, № 2. P. 107–115.
17. Sergeichik V., Ivaniuk A. Hardware Primitives for FPGA Design Obfuscation // Proceedings of the Section of Young Researchers and Scientists (SYRAS) on the 10th International Conference on Digital Technologies 2014. Zilina, Slovakia, 9–11 July 2014. P. 39–44.
18. Sergejchik V.V., Ivanjuk A.A. Osobennosti obfuskacii VHDL-opisanij i metody ocenki ee slozhnosti // Informatika. 2014. № 1 (41). S. 116–125. (in Russ.)

Сведения об авторах

Иванюк А.А., д.т.н., доцент, профессор кафедры информатики Белорусского государственного университета информатики и радиоэлектроники.

Заливако С.С., к.т.н., доцент кафедры информатики 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. +375-17-293-80-20;
e-mail: ivaniuk@bsuir.by
Иванюк Александр Александрович

Information about the authors

Ivaniuk A.A., D.Sci, associate professor, professor of computer science department of Belarusian state university of informatics and radioelectronics.

Zalivaka S.S., PhD, associate professor of computer science department of 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. +375-17-293-80-20;
e-mail: ivaniuk@bsuir.by
Ivaniuk Alexander Alexandrovich