УДК

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ, ПОСТРОЕННЫХ НА БАЗЕ КОМБИНИРОВАННОГО ГЕНЕРАТОРА

Кайкы М.Н.

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

Иванюк А.А. – доктор тех. наук, профессор каф. Информатики

Данная работа направлена на исследование характеристик случайности и уникальности физически неклонируемых функций, построенных на основе схемы комбинированного генератора. В работе рассмотрены структура схемы комбинированного генератора и режимы его работы. Представлены экспериментальные результаты, полученные при исследовании характеристик рассматриваемого типа физически неклонируемых функций на различных экземплярах программируемых логических интегральных схем - ПЛИС Xilinx семейства Zynq7000.

Введение.

В повседневной жизни люди используют электронные устройства для совершения покупок, перевода денег, записи информации. В компаниях и банках данные обрабатываются и хранятся электронным оборудованием. К сожалению, как и программное обеспечение, аппаратное обеспечение имеет высокие риски в области безопасности. Безопасность цифровых устройств – по сей день является актуальной темой для большинства людей и компаний, принимающих участие в цифровизации современного общества. Поскольку масштабы интегральных схем (ИС) быстро растут, а режим производства становится более гибким, основные проблемы безопасности ИС связаны с внедрением вредоносных схем, называемых аппаратными троянами (Hardware Trojan) [1]. С целью повышения уровня безопасности современных ИС, а также недопущению несанкционированного использования последних – применяются методы аппаратной идентификации и аутентификации, использующие методы физической криптографии для получения неповторимых и уникальных последовательностей. Данные последовательности могут выступать как в роли идентификатора цифрового устройства, так и в качестве источника энтропии, например для генерации закрытых ключей в алгоритмах шифрования. Для получения описанных последовательностей современные методы физической криптографии применяют понятие физически неклонируемых функций (ФНФ), впервые описанных в работе [2]. В данном исследовании, рассматривается возможность применения одной из реализаций ФНФ на базе ячеек комбинированного генератора случайных чисел, предложенных в работе [3].

Комбинированный генератор на базе нескольких ФНФ.

В работе [3], предлагается подход к построению генераторов истинно случайных чисел, предлагая совместить в одной базовой схеме генератора различные структуры физически неклонируемых функций. Как известно, каждая схема ФНФ обладает своими свойствами и особенностями [4, 5]. Комбинированная схема (Рис. 1), совмещает в себе такие виды ФНФ – статическая память, кольцевой генератор и элемент постобработки на базе Т-триггера.

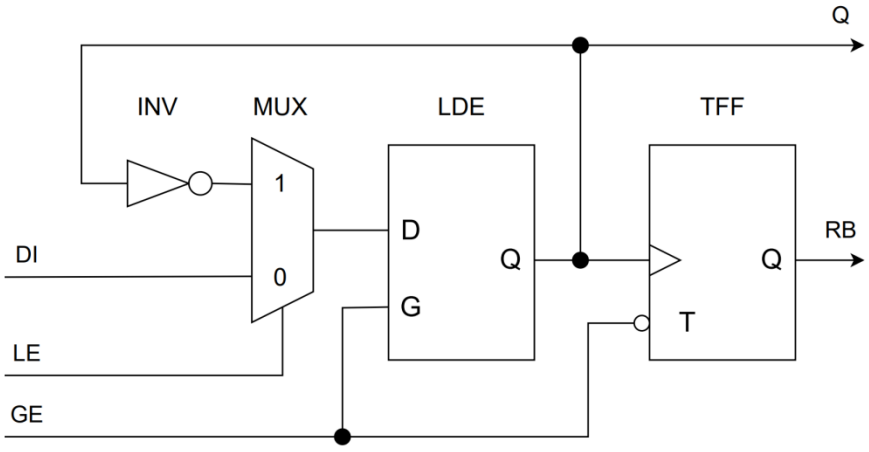

Рисунок 1 – Схема базового элемента комбинированного генератора

Данная схема базового элемента комбинированного генератора может работать в четырёх режимах:

1. *Режим загрузки данных.* При установке управляющих сигналов LE = 0 и GE = 1, значение, поданное на вход DI будет записано в триггер LDE и отображено на выходе Q. При этом, критический путь для записи будет обусловлен не только временами предустановки и удержания триггера LDE, а и логическими вентилями, образующими мультиплексор, что снижает максимально возможную частоту работы данной схемы в качестве запоминающего устройства.
2. *Режим кольцевого осциллятора.* При переходе в данный режим работы (LE = 1, GE = 1), базовый элемент комбинированного генератора начинает вырабатывать на выходе Q значения, изменяемые с частотой F_Q, определяемой задержками распространения сигнала через структуру элемента. Такое поведение обусловлено комбинационной обратной связью по пути INV → MUX → LDE → INV.
3. *Режим хранения данных.* (GE = 1 → 0, LE = 0) Данный режим необходим для фиксации данных, полученных в режиме загрузки или кольцевого осциллятора.
4. *Режим инициализации.* При включении питания на экземпляре цифрового устройства, и управляющего сигнала GE = 0 схема будет находится в режиме инициализации, что приведёт к её функционированию как ФНФ статической памяти.

Экспериментальная установка.

Для проведения экспериментальной части исследования характеристик физически неклонируемой функции на базе базовых элементов, предложенных в работе [3], была спроектирована цифровая система на базе программируемой логической интегральной микросхемы (ПЛИС) компании Xilinx – ZYNQ7000 [6], кристалл – xc7z010clg400-1. Выбранный кристалл ПЛИС располагался на отладочной плате, разработанной компанией Digilent – Zybo Z7 [7]. Для получения доступа к расположенным на элементной базе ПЛИС физически неклонируемым функциям была разработана IP компонента, позволяющая передавать на ФНФ входные последовательности от хост-процессора при помощи интерфейса AXI4-Lite. Также, в состав IP компоненты был добавлен набор устройств фиксации результата и систему анализа частот для каждого выхода генератора. Полученные в результате экспериментов данные обрабатывались встроенным в кристалл ПЛИС процессором ARM Cortex-A9, а затем передавались на рабочую станцию при помощи интерфейса UART со скоростью передачи 115200 бод и моста USB – UART на базе микросхемы конвертера FT2232. Схема генератора и описанных выше систем была описана на языке SystemVerilog и использованием готового решения от компании Xilinx – AXI4 BRAM Controller в виде подключаемой к проекту IP компоненты, структурная схема экспериментальной установки изображена на рисунке 2. Всего в эксперименте принимало участие
$N = 32$ базовых элемента. Для контроля частот работы элементов в режиме кольцевого генератора была применена схема с двумя счётчиками – счётчик импульсов и счётчик временного окна, схема их подключения к базовому элементу приведена на рисунке 3. При функционировании элемента в режиме КО – импульсы с выхода Q поступают на вход счётчика импульсов до тех пор, пока тот не перейдёт в своё конечное состояние счёта ($counter = 2^{32} - 1$) или пока счётчик временного окна не достигнет заданного хост-контроллером значения. Всего, для размещения экспериментальной установки на кристалле, при $N = 32$ понадобилось 4334 6-ти входовых таблиц истинности (LUT) и 3425 триггеров.

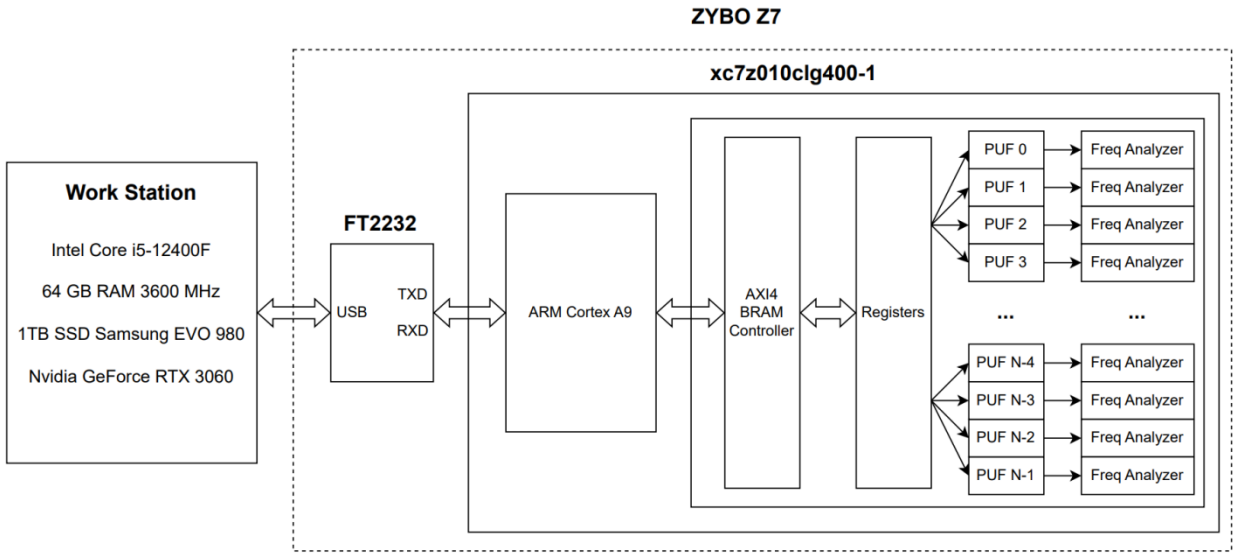

Рисунок 2 – Схема экспериментальной установки на базе ПЛИС

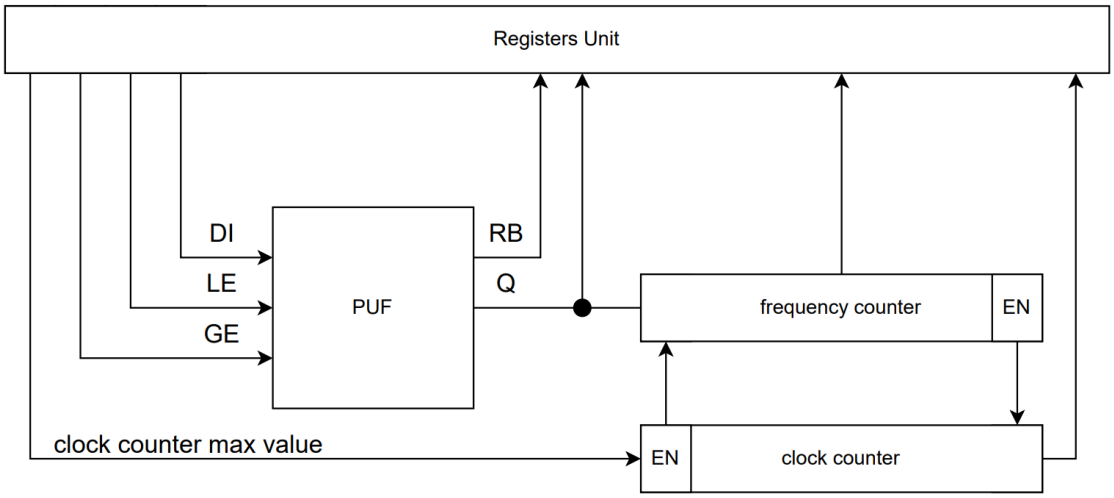

Рисунок 3 – Схема подключения анализатора частот к базовому элементу

Ход проведения эксперимента.

В ходе проведения ряда экспериментов были получены выходные последовательности набора базовых элементов комбинированного генератора, работающего в режимах инициализации и кольцевого генератора.

В первом эксперименте, при анализе данных, полученных в режиме инициализации оценивалась встречаемость единичного символа (*P*) выходе Q для каждого из базовых элементов (*N*). Для этого, были произведены циклы перезагрузки платы с ПЛИС, при помощи TCL скрипта, работающего в режиме отладки процессорного ядра ARM Cortex-A9. В результате проведения данного эксперимента был получен набор инициализационных значений для каждой ячейки в зависимости от номера цикла перезагрузки экземпляра ПЛИС, который позволил построить тепловую карту значений при инициализации – рисунок 4.

N	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
P_0	1.0	1.0	0	0	0	1.0	1.0	0	0	0	1.0	0	0	0.67	0	1.0	1.0	0	0	1.0	0	1.0	0	0	1.0	0	0	0.94	1.0	0	0	1.0
$P1$	1.0	1.0	1.0	0.19	0	1.0	0	0	1.0	0	1.0	0	0	0.83	0	1.0	1.0	0	0	0	0	1.0	0	1.0	1.0	0	0	1.0	1.0	0	1.0	1.0

Рисунок 4 – Тепловая карта инициализационных значений для двух реализованных систем

Для полученных данных проведем оценку основных характеристик ФНФ: стабильность, уникальность, единообразие. Как видно из рисунка 4, большинство базовых элементов являются

стабильными – 93.75% ячеек не изменяют своих значений в зависимости от цикла перезапуска. Такое поведение связано непосредственно со структурой бистабильного элемента на базе асинхронного *D*-триггера и наличием асимметрии в его реализации, а меньшая асимметрия приводит к попаданию схемы в метастабильное состояние, что доказывают значения $0 < P < 1$ [3].

В результате проведения оценки стабильности полученных идентификаторов были сформированы два базовых вектора по мажоритарному правилу:

$V = \{id_0, id_1, id_2, \dots, id_{N-1}\}$, где $id_i = 0$, если $P_i < 0{,}5$, иначе $id_i = 1$, i – номер разряда в идентификаторе.

Для оценки уникальности будем использовать удельное расстояние по Хэммингу (HD) (формула 1) между данными векторами.

$$Uniq = \frac{1}{N} HD(V_0, V_1) \quad (1),$$

где HD – расстояние по Хэммингу между векторами V_0 и V_1 разрядности N, где V_0 – идентификатор, полученный на первом экземпляре ПЛИС, V_1 – на втором. В результате анализа было получено среднее значение метрики межкристальной уникальности $HD = 0{,}1875$ между полученными идентификаторами в процессе проведения эксперимента.

Расчёт метрики единообразия проводился по формуле 2, данная метрика отражает соотношения нулей и единиц в каждом из полученных идентификаторов.

$$U_i = 100 \times \left(1 - 2 \times \left|\frac{WH(V_i)}{N}\right|\right)\% \quad (2),$$

где $WH(V_i)$ – вес бинарного вектора V по Хэммингу; i – номер экземпляра ПЛИС; N – разрядность вектора (идентификатора). Среднее единообразие составило: $U_0 = 93.78\%$ $U_1 = 98.12\%$

Вторым этапом проведения экспериментов стало изучение значений частот работы кольцевых генераторов, имеющихся в структуре базовых элементов. Для этого, базовые элементы переводились хост-процессором в режим КО во временном окне $W = k \times P_{SYS\_CLK} = 1.19$ мс для двух экземпляров генератора, где *k* – регулируемый коэффициент масштабирования (максимальное значение счётчика тактов), P_{SYS_CLK} - период системного синхросигнала, равного 100 МГц. Результаты измеренных частот приведены на рисунке 5. Измерения проводились при последовательном переключении генератора из режима инициализации в режим КО на временное окно *W* и далее в режим сохранения данных.

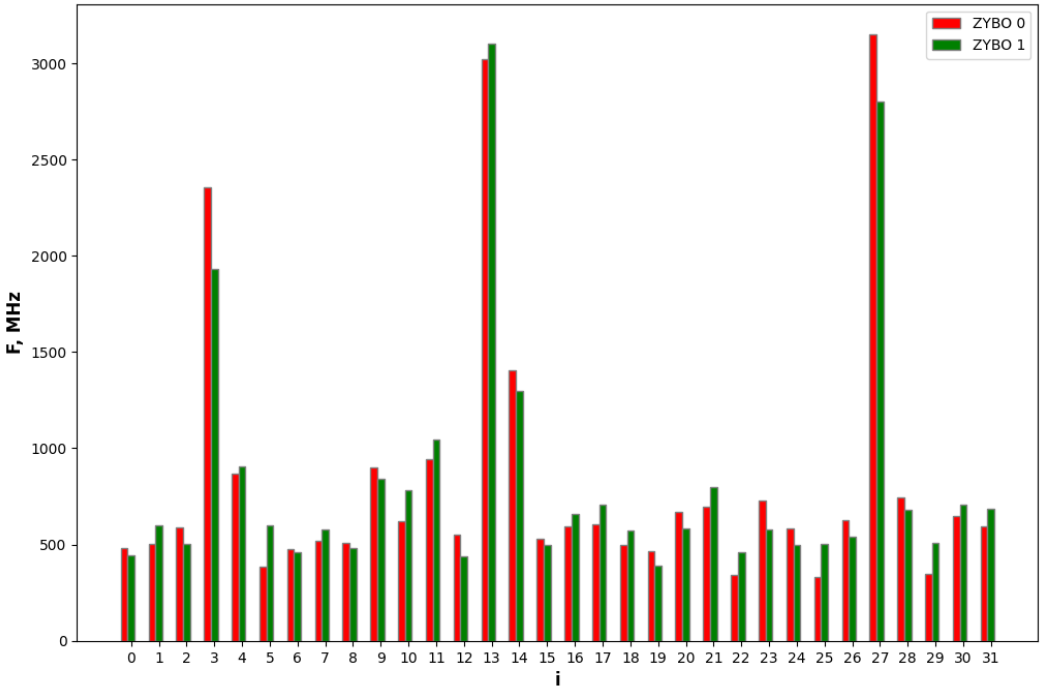

Рисунок 5 – Значения измеренных частот на двух различных экземплярах ПЛИС

Присутствующие выбросы на разрядах **3**, **13**, **27** можно связать с высокочастотными колебаниями на выходе Q базовых элементов, которые привели к аномальному функционированию измеряющих счётчиков, также, можно заметить, что данные выбросы были зарегистрированы на ячейках, имеющих низкую стабильность в режиме инициализации, что также подтверждает данную гипотезу в виду высокой степени симметрии полученных структур.

Как упоминается в работах [8, 9], подобные высокочастотные колебания на информационном входе триггера/защёлки способны вводить его в метастабильное состояние, имеющее форму затухающих автоколебаний. Так как реализация аналого-цифровых преобразователей высокого разрешения внутри современных интегральных микросхем по сей день является трудно решаемой задачей, а в исследуемых образцах ИС отсутствуют системы регистрации сигналов со схожими АЦП характеристиками, было предложено регистрировать подобные автоколебания при помощи счётчиков передних фронтов сигналов.

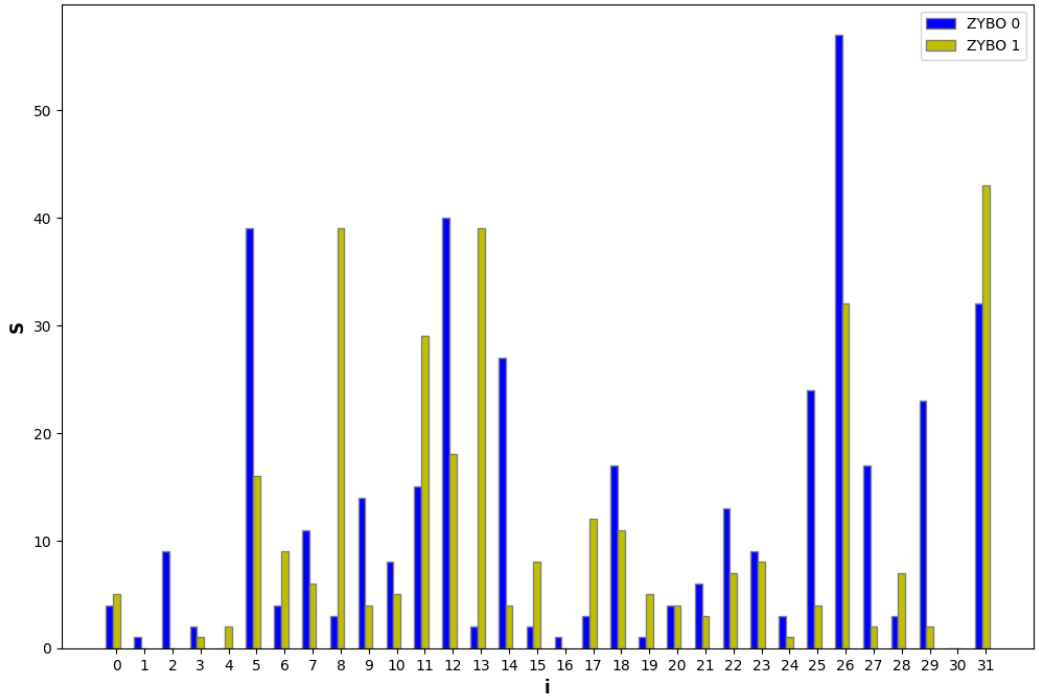

Рисунок 6 – Средние значения количества фронтов автоколебаний

Для регистрации данного эффекта автоколебаний, разработанные ячейки ФНФ переводились в режим функционирования как кольцевые осцилляторы во временном окне равном 1.19 мс, затем, режим работы изменялся на режим хранения с включением систем регистрации передних фронтов на временное окно 600 мс. Данное временное окно было выбрано исходя из времени переходного процесса на триггере – мы не можем знать точное время выхода триггера из метастабильного состояния, поэтому регистрируем фронты колебаний как можно дольше, с целью убедится в том, что все триггеры перешли в устойчивое состояние. На рисунке 6 приведены полученные в результате эксперимента средние значения количества фронтов автоколебаний для каждой ячейки и экземпляра ПЛИС. Как видно из рисунка 6, почти все ячейки ФНФ генерировали автоколебательные процессы на выходе Q, что подтверждает гипотезу о колебательных процессах в защёлке при нарушении параметров предустановки и удержания входных данных. Стоит отметить, что все элементы ФНФ, участвующие в экспериментах, в конечном итоге пришли к своему стабильному состоянию, что также подтверждает гипотезу о форме колебаний как затухающих.

Заключение.

В результате проведения исследований характеристик физически неклонируемых функций на базе предложенного в работе [3] комбинированного генератора были получены значения стабильности, уникальности и единообразия для базовых ячеек ФНФ, работающих в режиме инициализации, а также измерены частоты колебаний данных ячеек в режиме работы как кольцевые осцилляторы. В режиме инициализации полученные структуры ведут себя свойственно статической памяти и обладают схожими с ней характеристиками [10], они достаточно стабильны между перезагрузками (93.75%), имеют хорошие показатели единообразия ($U_0 = 93.78\%$ $U_1 = 98.12\%$). В режиме работы в качестве кольцевого осциллятора базовые элементы показывают среднее значение частот колебаний равное 821 и 818 МГц для каждого из экземпляров ПЛИС, однако наблюдались и высокочастотные выбросы, приводящие к сбоям в работе измеряющих структур. Как показали проведённые эксперименты, базовые ячейки, предложенные в работе [3] – могут выступать как в качестве источников энтропии для генераторов случайных чисел, так и как идентификаторы в аппаратном обеспечении. Отдельно стоит обратить внимание на третью часть эксперимента – исследование эффекта автоколебательных процессов при завершении работы базового элемента в режиме кольцевого генератора. При переходе из режима работы КО в режим хранения данных, защёлка LDE переходила в режим метастабильности с генерацией колебательных процессов на её выходе. Полученный эффект остаточных колебаний связан непосредственно с ассиметричной структурой D-защёлки, и позволяет получать неконтролируемые, уникальные для каждого экземпляра, затухающие колебания на выходе базового элемента. Данные колебания могут стать основой для будущих систем генерации истинно случайных чисел, так как не подвержены прямому влиянию управляющей системы и обладают высокой степенью уникальности.

Список использованных источников:

1. Sumathi G., Srivani L., Murthy D.T., Madhusoodanan K., Murty S.A.V.S. A Review on HT Attacks in PLD and ASIC Designs with Potential Defence Solutions. IETE Tech. Rev. 2018; 35:64–77. [Google Scholar]

2. Pappu, R. Physical One-Way Functions: Ph.D. thesis / R. Pappu // MIT. – Boston, USA, 2001.

3. Иванюк А.А. Комбинированный генератор случайных чисел на программируемых логических интегральных схемах. Цифровая трансформация. 2023;29(1):36-47. https://doi.org/10.35596/1729-7648-2023-29-1-36-47

4. Claes, M., van der Leest, V., Braeken, A. (2012). Comparison of SRAM and FF PUF in 65nm Technology. In: Laud, P. (eds) Information Security Technology for Applications. NordSec 2011. Lecture Notes in Computer Science, vol 7161. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-29615-4_5

5. Abhranil Maiti, Vikash Gunreddy, and Patrick Schaumont. A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions https://eprint.iacr.org/2011/657.pdf

6. Семейство ПЛИС – ZYNQ7000 [Электронный ресурс]. – Режим доступа: https://www.xilinx.com/products/silicon-devices/soc/zynq-7000.html. – Дата доступа - 15.03.2023

7. Отладочная плата на базе ПЛИС – ZYBO Z7 [Электронный ресурс]. – Режим доступа: https://digilent.com/reference/programmable-logic/zybo-z7/start – Дата доступа - 15.03.2023

8. Kacprzak T. (1988) Analysis of Oscillatory Metastable Operation of an RS Flip-Flop. IEEE Journal of Solid-State Circuits. 23 (1), 260–266.

9. Zalivaka S. S., Ivaniuk A. A., Chang Ch. H. (2018) Reliable and Modeling Attack Resistant Authentication of Arbiter PUF in FPGA Implementation with Trinary Quadruple Response. IEEE Transactions on Information Forensics and Security. 14 (4), 1109–1123.

10. Кайкы, М. Н. Сравнение характеристик ФНФ статической памяти с использованием плис и промышленных микросхем = Comparison of static memory puf characteristics using FPGA and industrial Ics / М. Н. Кайкы, А. А. Иванюк // Приборостроение-2022 : материалы 15-й Международной научно-технической конференции, 16-18 ноября 2022 года, Минск, Республика Беларусь / редкол.: О. К. Гусев (председатель) [и др.]. – Минск: БНТУ, 2022. – С. 37-39.

UDC

INVESTIGATION OF THE CHARACTERISTICS OF A PHYSICALLY UNCLONABLE FUNCTION BUILT ON THE BASIS OF A COMBINED GENERATOR

Kaiky M.

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

Ivaniuk A.A. – Dr. of Sci. (Eng.), Associate Professor, Professor at the Comp. Sci. Department

This work is aimed at studying the characteristics of randomness and uniqueness of a physically uncloneable function built on the basis of a combined generator circuit. The paper considers the structure of the combined generator circuit and its operating modes. Experimental results obtained in the study of the characteristics of this physically uncloneable function on various copies of programmable logic integrated circuits - FPGA Xilinx of the Zynq7000 family are presented.