УДК *004.312*

МЕТОД ПОВЫШЕНИЯ УНИКАЛЬНОСТИ АППАРТНЫХ ИДЕНТИФИКАТОРОВ ПЛИС НА ОСНОВЕ ФИЗИЧЕСКИ НЕКЛОНИРУЕМЫХ ФУНКЦИЙ ТИПА КОНФИГУРИРУЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

Л.А. Бурко, А.А. Иванюк

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Беларусь

Аннотация. В работе рассматривается задача повышения уникальности аппаратных идентификаторов ПЛИС, которые формируются на основе физически неклонируемых функций типа конфигурируемого кольцевого осциллятора. Показано, что использование аддитивного скремблера для постобработки идентификаторов может приводить к возникновению совпадающих значений вследствие особенностей исходных идентификаторов и начального состояния генератора. Для устранения данной проблемы предложен метод предварительного преобразования исходных идентификаторов. Проведенные экспериментальные исследования показали повышение статистического разнообразия идентификаторов и снижение вероятности коллизий.
Ключевые слова: ПЛИС; ФНФ; ККО; аддитивный скремблер; идентификация; LFSR; переключательная активность; защита аппаратуры; расстояние Хэмминга.

METHOD FOR INCREASING THE UNIQUENESS OF FPGA HARDWARE IDENTIFIERS BASED ON PHYSICALLY UNCLONABLE FUNCTIONS OF CONFIGURABLE RING OSCILLATORS

L.A. Burko, A.A. Ivaniuk
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This article examines the problem of increasing the uniqueness of hardware identifiers for FPGA devices generated using physically unclonable functions based on configurable ring oscillators. Using an additive scrambler for identifier postprocessing can lead to collisions due to the characteristics of the original identifiers and the initial state of the generator. To overcome this issue, a method for pre-transforming the original identifiers is proposed. Experimental studies have demonstrated an increase in the statistical diversity of identifiers and a reduction of collisions.
Keywords: FPGA; PUF; CRO; additive scrambler; identification; LFSR; switching activity; hardware protection; Hamming distance.

Введение

Аппаратные методы обеспечения безопасности играют важную роль в современных информационно-телекоммуникационных системах. Их используют при реализации вычислительных и криптографических функций наряду с программными механизмами защиты информации, что позволяет повысить уровень доверия к устройствам и предотвратить несанкционированное вмешательство. Одной из ключевых задач в области защиты информации является идентификация и аутентификация аппаратных компонентов. Особую актуальность эта задача приобретает для устройств, реализованных на базе ПЛИС, широко применяемых в системах обработки сигналов, телекоммуникационном оборудовании, встроенных вычислительных системах и средствах криптографической защиты информации благодаря высокой гибкости архитектуры и возможности динамической реконфигурации. Программируемая природа таких устройств создает риски подмены аппаратных модулей,

клонирования устройств или внедрения несанкционированных модификаций в конфигурацию системы.

Эффективным способом повышения уровня защищенности аппаратных платформ является использование уникальных аппаратных идентификаторов [1, 2]. В отличие от идентификаторов, хранящихся в энергонезависимой памяти, они могут формироваться на основе внутренних характеристик микросхемы, что существенно усложняет копирование или подмену устройств.

Основная часть

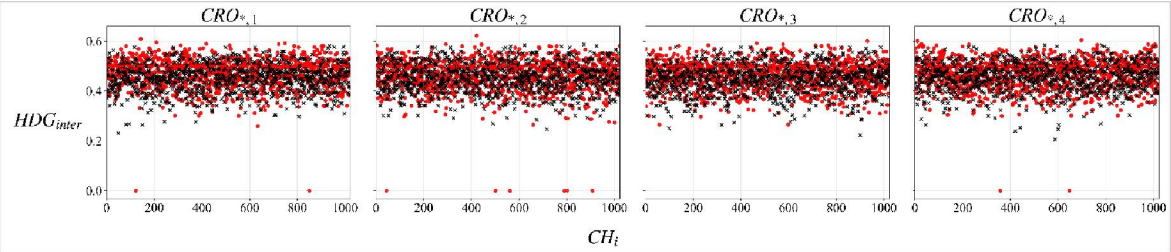
Процесс формирования идентификаторов на базе физически неклонируемых функций (ФНФ) для ПЛИС был подробно описан в [2]. Степень различия идентификаторов оценивается на основе метрики геометрического среднего расстояний Хэмминга. Эксперимент был проведены на четырех различных ПЛИС, на каждой из которых было реализовано по четыре экземпляра ФНФ ККО с фиксированными параметрами, которые влияют на длину идентификатора. Полученные идентификаторы различны, но их статистические характеристики остаются недостаточными для обеспечения требуемого уровня метрики уникальности. Была предложена схема улучшения идентификаторов на основе аддитивного скремблера. При оценке уникальности идентификаторов после постобработки возникла проблема появления повторяющихся идентификаторов.

Новое значение идентификатора ID_i^* генерируется при помощи аддитивной схемы путем применения операции xor между первоначальным значением идентификатора ID_i и начальным значением LFSR, входящего в состав скремблера. Разрядность LFSR n совпадает с длиной идентификатора. Важно, чтобы инициализирующее значение генератора было уникальным для каждой пары ПЛИС – ФНФ ККО, поэтому оно формируется путем конкатенации бинарных представлений индексов компонентов (ПЛИС и ФНФ ККО) расширенное нулями до размера n. Например, для ПЛИС с индексом 2 и ФНФ ККО с индексом 3 начальное значение – 000010|0000011. Так как начальные значения содержат большую часть нулей, необходимо осуществить дополнительных K сдвигов LFSR в режиме генератора ($K > n$), таким образом получится новое значение $LFSR_i$.

Пусть даны ID_1 и ID_2, $LFSR_1$ и $LFSR_2$. Если $ID_1 \oplus LFSR_1 = ID_2 \oplus LFSR_2$, то значение метрики уникальности будет равняться 0. Например, ID_1 = 110**1**00**0**01**1**000 и ID_2 = 110**0**00**1**01**0**000, $LFSR_1$ = 110**1**01**0**00**0**001 и $LFSR_2$ = 110**0**01**1**00**1**001, отличительные позиции одинаковые. Из-за наблюдаемой коллизии между значениями идентификаторов и значениями LFSR получится нулевое значение метрики уникальности. Способом увеличения расстояния между идентификаторами является их

преобразование в последовательности переходов между соседними битами. Каждая пара заменяется по правилу: 00 → 0, 01 → 1, 10 → 1, 11 → 0. Применив это, получаются новые начальные идентификаторы 01**11**0**00**1**01**001 и 01**00**0**11**1**10**001, отличные на 6 разрядов. После применения аддитивного скремблера получатся значения идентификаторов 10**1**00**1**01**0**1000 и 10**0**00**0**01**1**1000.

В эксперименте было использовано $K = 50$ и измерялась межкристальная уникальность. Красные точки – значения уникальности для идентификаторов после аддитивной схемы без стартовых модификаций, черные крестики – с стартовой модификацией. Общее количество нулевых значений снизилось с 10 до 0. Среднее значение метрики уникальности новых идентификаторов по сравнению с начальными выросло с 0,4023 до 0,4530 (максимальное значение 0,5).



Значения метрик уникальности для идентификаторов
Uniqueness metric values for identifiers

Заключение

Формирование уникальных идентификаторов на аппаратном уровне позволяет повысить устойчивость ПЛИС к атакам, связанным с копированием или подменой устройств. В работе предложен улучшенный подход к генерации уникальных идентификаторов, основанный на предварительном преобразовании исходных идентификаторов на основе переходов между соседними битами перед их использованием в аддитивном скремблере. Это позволяет увеличить различие между начальными последовательностями, что приводит к повышению статистического разнообразия генерируемых идентификаторов и снижению вероятности возникновения совпадающих значений.

Список использованных источников

1. Иванюк, А. А., Бурко Л.А. (2025) Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого. *Информатика*. 22(4) 65–81.

2. Ivaniuk, A., Burko L. (2025) Unclonable Identification and True Random Number Generation Based on CRO PUF. *Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference*, 103-107.

References

1. Ivaniuk, A. A., Burko L.A. (2025) Generation of deterministic identifiers and random numbers using a configurable ring oscillator circuit. *Informatics*. 22(4), 65–81 (in Russian).

2. Ivaniuk, A., Burko L. (2025) Unclonable Identification and True Random Number Generation Based on CRO PUF. *Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference*, 103-107.

Сведения об авторах

Бурко Л.А., магистрант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», burkoliana@gmail.com.

Иванюк А.А., д.т.н., профессор кафедры информатики, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», ivaniuk@bsuir.by.

Information about the authors

Burko L.A., Master Student, Educational Institution "Belarusian State University of Informatics and Radioelectronics", burkoliana@gmail.com.

Ivaniuk A.A., D.Sci, Professor of Informatics Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", ivaniuk@bsuir.by.