ИССЛЕДОВАНИЕ ПОВЕДЕНИЯ КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

Бурко Л. А., Иванюк А. А.
Кафедра информатики, Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: burkoliana@gmail.com, ivaniuk@bsuir.by

В статье рассматривается поведение физически неклонируемых функций (ФНФ) на базе кольцевых осцилляторов (КО), которые предлагают значительное улучшение в области аппаратной защиты данных и идентификации.

Введение

Существует множество способов создать уникальные идентификаторы и генераторы случайных чисел. Большинство из них имеют сложную аппаратную реализацию. Одним из способов решения данной проблемы может быть схема со счётчиком, которая действительно может быть основой для реализации физически неклонируемой функции (ФНФ) на базе кольцевого осциллятора (КО). Эта конструкция позволяет создать уникальные сигнатуры для каждого устройства, опираясь на физические особенности конкретного экземпляра схемы. Это позволяет использовать КО-ФНФ для криптографических задач и защиты интеллектуальной собственности, предлагая отличные статистические характеристики и устойчивость к технологическим вариациям [1-2].

I. Описание структуры КО

ФНФ описываются значениями пар входных и соответствующих им выходных параметров (сигналов). Подобная пара, состоящая из входного физического параметра (запроса) и выходного параметра (ответа), называется парой запрос – ответ [3]. Важными параметрами являются частотный диапазон КО, временное окно измерения частоты и разрядность счетчика измерения.

Для эксперимента были взяты 4 платы Digilent Zybo-Z7, в каждой размещено по 4 КО.

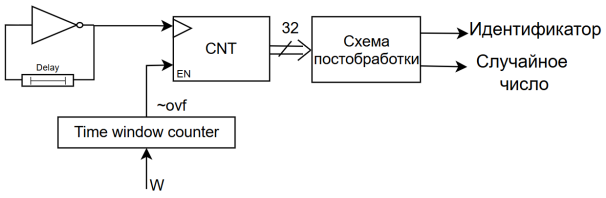

Рис. 1 – Схема генерации случайного числа и уникального аппаратного идентификатора

II. Описание эксперимента

Эксперимент состоит в получении и исследовании характеристик генерируемых частотных значений. Для анализа были сняты 32 набора данных по миллиону частотных значений.

В фиксированном окне измерения значения счетчика можно условно поделить на 3 зоны:

1. Стабильная зона, где на повторяющихся экспериментах значения разрядов не изменяются (на рис.2 это [0-6]). На данной зоне выполняются условия $p(1)=0$ или $p(1)=1$, где p это вероятность.

2. Две метастабильных зоны, одну можно назвать сильной ([11-23]), вторую слабой([7-10]). На сильной зоне вероятность появления *0* или *1* на определенной позиции стремится к $p=0.5$. Существует вопрос, какое отклонение считать нормальным. На данном этапе эксперимента отклонение было принято $e=0.03$. После первого значения неудовлетворяющего условию начинается слабая зона.

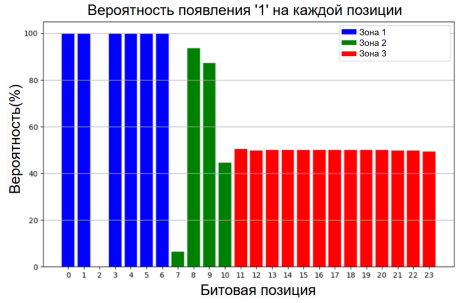

Рис. 2 – Гистограмма вероятностей появления единицы на каждой битовой позиции

На рисунке 3 показано распределение сильной метастабильной зоны.

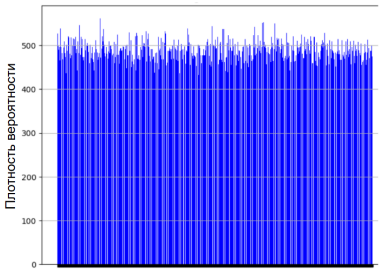

Рис. 3 – Распределение сильной метастибльной зоны

III. Влияние временного окна на размер зон

Счетчик собирает количество изменений сигнала *clk* за временное окно *W*. Итого результатом

Работа выполнена в совместной учебной лаборатории БГУИР-YADRO
https://www.bsuir.by/ru/kaf-informatiki/yadro

ответа является значение N. Вследствие неконтролируемых вариаций технологических процессов при изготовлении интегральной схемы значение N каждый раз будет меняться.

В ходе эксперимента, было выявлено, что длина стабильной и метастабильной частей отличаются. Для одной конфигурации были выбраны различные временные окна. Из рисунка 4 следует, что с увеличением окна увеличивается размер метастабильной и стабильной зон.

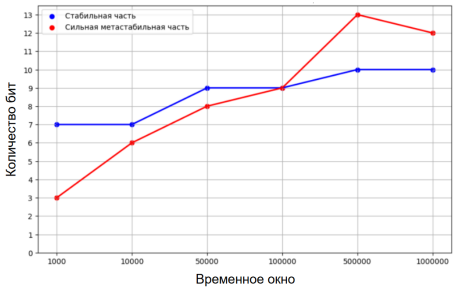

Рис. 4 – График распределения длины уникального идентификатора и сильной метастабильной зоны

Минимальная длина уникального идентификатора для разрядности 32 изменялась с четырех бит до восьми. С увеличением периода длина сильной метастабильной части увеличивается.

IV. Интер- и интра-уникальность

На рисунке 5 показаны идентификаторы, т.е. стабильные многоразрядные ответы, исследуемых ПЛИС. Черным цветом обозначены «элементы памяти», которые сохраняют значение 1 в результате 1000000 измерений, белым — сохраняющие значение 0. Для каждой пары среди стабильных зон было посчитано удельное расстояние Хэмминга – количество различающихся позиций для строк с одинаковой длиной деленное на длину. Для выделения восьми бит были добавлены значения из слабой метастабильной зоны по мажоритарному признаку. Интра-уникальность – среднее значение расстояний Хэмминга для каждой из ПЛИС. Интер-уникальность – среднее значение расстояний Хэмминга для каждого из каналов среди различных ПЛИС. Результаты представлены в таблице 1. *CH0-CH3* – каналы.

Таблица 1 – Удельное расстояние Хэмминга

Интра-уникальность		Интер-уникальность	
ПЛИС1	0.5	CH0	0.459
ПЛИС2	0.375	CH1	0.417
ПЛИС3	0.395	CH2	0.479
ПЛИС4	0.459	CH3	0.375

Построенные таким образом идентификаторы обладают достаточно высокими значениями внутри и межкристалльной уникальности.

V. Вывод

Реализация ФНФ на КО представляет собой простое и эффективное схемотехническое решение, которое позволяет решать две ключевые задачи: для целей идентификации можно использовать сильную детерминированную зону, а для генерации случайных чисел – метастабильную зону, которая более чувствительна к случайным воздействиям и менее предсказуема.

В процессе исследования было установлено, что параметры зон существенно зависят от размера временного окна и рабочей частоты. Таким образом, баланс между размером окна и частотой работы позволяет гибко настраивать параметры ФНФ для оптимизации работы как в режиме идентификации, так и в режиме генерации случайных чисел, что делает данное решение универсальным для различных приложений, связанных с безопасностью и защитой данных.

VI. Список литературы

1. А. А. Иванюк, Применение конфигурируемых генераторов импульсов для идентификации ПЛИС. Информатика. 2011; (4(32)):113-123. `https://inf.grid.by/jour/article/view/343?locale=ru_RU`
2. А. А. Иванюк, В. Н. Ярмолик, Физически неклонируемые функции на базе управляемого кольцевого осциллятора. Безопасность информационных технологий. 2023; (3(30)):90–103 `https://bit.spels.ru/index.php/bit/article/view/1532`
3. В. Н. Ярмолик, Ю.Г. Вашинко, Физически неклонируемые функции. Информатика. 2011; (2(30)):90–100. `https://inf.grid.by/jour/article/view/370?locale=ru_RU`

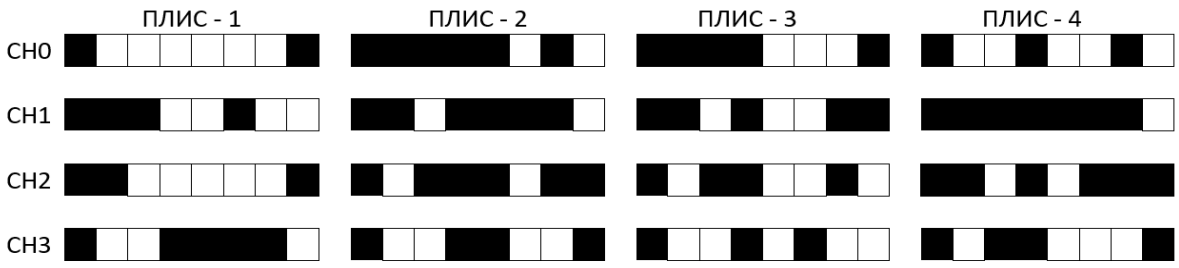

Рис. 5 – Идентификаторы для исследуемых ПЛИС