ГЕНЕРАЦИЯ СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ СХЕМЫ ФНФ КОНФИГУРИРУЕМОГО КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА

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

В статье исследуется поведение физически неклонируемых функций (ФНФ), реализованных на основе конфигурируемого кольцевого осциллятора (ККО). Такие структуры позволяют эффективно решать задачи аппаратной идентификации и генерации случайных чисел при минимальных затратах вычислительных и схемотехнических ресурсов. Представленные результаты показывают, что поведение ФНФ на базе ККО обладает выраженной стохастической природой, что подтверждает их пригодность для использования в системах, требующих высокой степени случайности и устойчивости к клонированию.

Введение

Современные информационные системы предъявляют всё более высокие требования к безопасности, аутентификации и защите данных. Одним из перспективных направлений в этой области является использование физически неклонируемых функций (ФНФ) [1], основанных на естественных вариациях физических параметров микросхем. Особый интерес представляют ФНФ, реализованные на основе конфигурируемых кольцевых осцилляторов (ККО), так как они имеют простую аппаратную реализацию, обладают высокой скоростью работы и способны формировать устойчивые уникальные отклики. Такие структуры позволяют создавать уникальные аппаратные идентификаторы, которые невозможно воспроизвести даже при полном копировании технологии изготовления устройства. Так же, помимо задач идентификации [2], ФНФ на базе ККО могут служить источником аппаратной случайности, что делает их эффективными для применения в генераторах случайных чисел и криптографических протоколах.

I. Описание эксперимента

Схема эксперимента (рисунок 1) более подробно уже была описана в предыдущем исследовании[2].

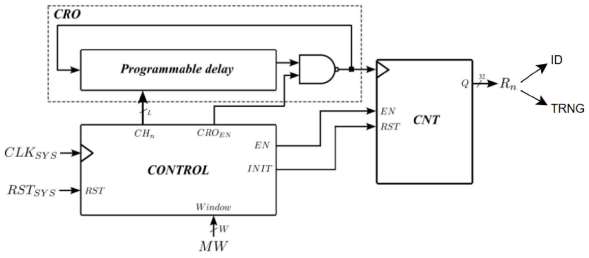

Рис. 1 – Схема эксперимента

Для сбора данных в эксперименте использовалась плата быстрого прототипирования Digilent ZYBO Z7-10 (Xilinx Zynq-7000). ФНФ ККО формирует уникальный ответ R_n, характеризующийся различиями в последовательности выходных битов. При многократном количестве измерений счетчика, для всех значений можно выделить стабильную и нестабильную группу. На рисунке 2 отображены битовые вероятности поразрядно: черным цветом – $P_1 = 1$, белым – $P_1 = 0$, серым – $0{,}45 < P_1 < 0{,},55$, где P_1 – вероятность появления 1 на определенном разряде.

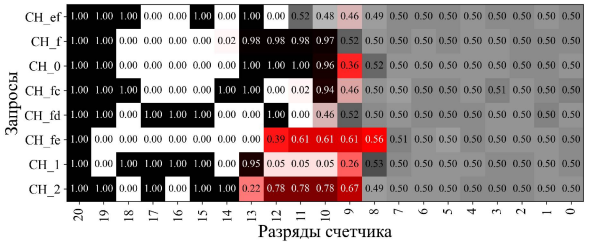

Рис. 2 – Битовые вероятности при различных CH_n

Стабильную часть можно использовать в качестве уникальных идентификаторов (значения красного цвета можно стабилизировать по мажоритарному принципу). Как показано на рисунке 2, при одинаковой прошивке ПЛИС, но при различных CH_n, получаются каждый раз различные идентификаторы. Схожесть имеют CH_0 и CH_f, но идентификатор для CH_f на 1 бит длиннее, тем самым видно, что все идентификаторы различны.

II. Уникальность ответов ФНФ

Нестабильная часть (биты серого цвета на рисунке 2) обладает свойствами равномерного распределения. Помимо этого, было выдвинуто предположение, что значения со счетчика являются уникальными и неповторимыми. Для проверки этого предположения были собраны 4 сета данных после перезапусков платы. Битовая последовательность собирается путем конкатенации значений счетчика, где $P_1 \approx 0{,}5$. Для графического отображения был использован Random Walk

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

2D (RW2) тест, для которого битовая последовательность делится на пары битов, и в зависимости от этого строится траектория движения («00» – влево, «01» – вверх, «10» – вправо, «11» – вниз). Результаты теста RW2 представлены на рис. 3. Видно, что все 4 траектории различны.

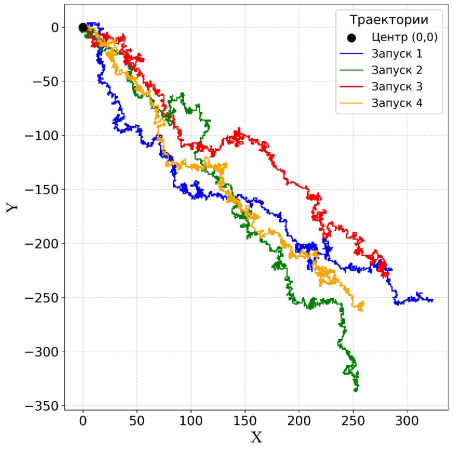

Рис. 3 – Траектории RW2 теста для различных перезапусков

III. Равномерность данных от ФНФ

Как видно из RW2 теста, преобладают подпоследовательности «11» и «10». Для визуальной проверки равномерности данных можно построить графический тест распределения точек на плоскости, для которого битовая последовательность делится на числа a_0,a_1,a_2 ... по 8 бит (количество бит может быть любое) и далее отображаются точки с координатами $(a_0,a_1),(a_1,a_2),\ldots$. На рисунке 4 (слева) видно, что для исходных данных со счетчика виден особый паттерн, но в дальнейшем, с примененением постобработки, от паттерна можно избавиться (рис. 4 (справа)). При проверке последовательностей на Health Tests из пакета NIST[3], прошел только Rank-тест. Тем самым, можно сделать вывод, что исходные данные от ФНФ ККО не могут являться хорошим источником случайности.

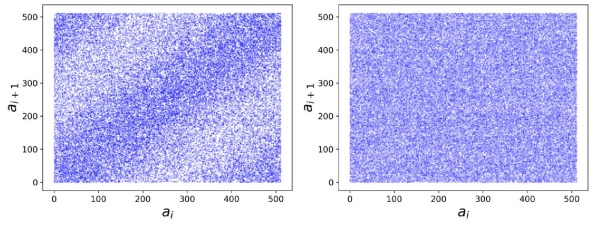

Рис. 4 – Результаты теста на распределение значений на плоскости

Разряды значений с вероятностью близкой к 0,5 (на рис.2 это разряды [7-0]) могут быть хорошей основой для источника случайных чисел. Для этого можно применить технологию постобработки, построенную на принципе регистра сдвига с линейной обратной связью.

Постобработка данных выполнялась с использованием схемы MISR (Multiple-Input Signature Register, многовходового регистра сигнатуры). Данная схема предназначена для объединения нескольких входных потоков данных (в рассматриваемом случае это разряды [7:0]) с целью формирования итоговой сигнатуры, являющейся свернутым представлением совокупного результата всех предшествующих операций. В качестве порождающего полинома использовался полином «1A7», соответствующий выражению $\varphi(x) = 1+x+x^2+x^3+x^6+x^8$. Как видно из RW2 теста на рисунке 5, данные после постобработки обладают достаточной визуальной случайностью.

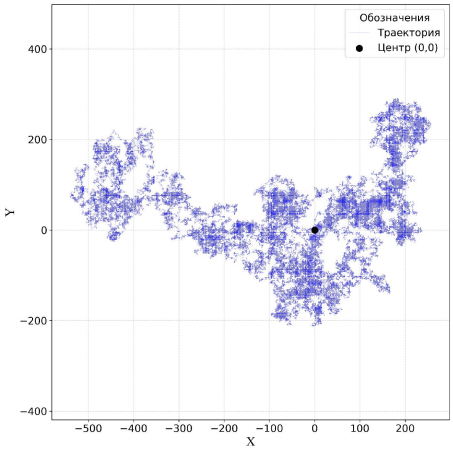

Рис. 5 – RW2 тест для значений с постобработкой

После постобработки прошли 12 из 13 тестов из пакета NIST и все 148 неперекрывающийся шаблонов. Не прошел тест Universal. Предполагается, что для его прохождения необходим больший объем данных.

IV. Вывод

В результате исследования было показано, что ФНФ ККО, при минимальном использовании аппаратных ресурсов, является хорошим источником идентификации, и при применении постобработки, может выступать надежным, уникальным источником случайных чисел, что подтверждают NIST-тесты и графическое отображение.

V. Список литературы

1. Иванюк, А. А. Исследование физически неклонируемой функции конфигурируемого кольцевого осциллятора / А. А. Иванюк // Информатика. – 2025. – Т. 22, № 1. – С. 73–89. – DOI: 10.37661/1816-0301-2025-22-1-73-89.
2. Unclonable Identification and True Random Number Generation Based on CRO PUF Pattern Recognition and Information Processing (PRIP'2025), Ivaniuk A, Burko L., Proceedings of the 17th International Conference, 16–18 Sept. 2025, Minsk, Belarus. – Minsk : UIIP NASB, 2025. – 496 p.
3. NIST 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation / `https://doi.org/10.6028/NIST.SP.800-90B`