

ИССЛЕДОВАНИЕ ФНФ КОЛЬЦЕВОГО ОСЦИЛЛЯТОРА КАК ИСТОЧНИКА СЛУЧАЙНОСТИ

Бурко Л.А.

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

Иванюк А.А. – д-р техн. наук, профессор

Данная работа описывает как физически неклонируемая функция (ФНФ) на базе кольцевого осциллятора (КО) может быть источником случайных чисел, а также манипуляции с дискретным нормальным распределением для выявления зависимостей между характеристиками распределения, и оценки некоторых параметров. Использовалась библиотека numpy языка Python.

Одним из способов получения как случайных чисел, так и уникального идентификатора является реализация физически неклонируемой функции на базе кольцевого осциллятора (ФНФ КО) [1]. Одно из достоинств этого метода – простота реализуемой схемы, рисунок 1. Идея данного метода уже была описана в предыдущем исследовании [2]. Каждый ФНФ КО, расположенный в различных местах ПЛИС, генерирует сигнал с уникальной частотой (периодом). В качестве количественной меры используется

число тактовых сигналов, регистрируемых счетчиком в фиксированном временном окне. R_i – значение двоичного счетчика в i -ом измерении. При переводе значений R_i в бинарный вид, где $i \in [0, m-1]$, m – количество проведенных измерений, предполагается разделение между стабильной (сигнал) и нестабильной (шум) частями. Наша задача – оценить предполагаемые границы шума (на рисунке 1 – биты n) и найти зависимости между характеристиками собранных с ФНФ КО данных.

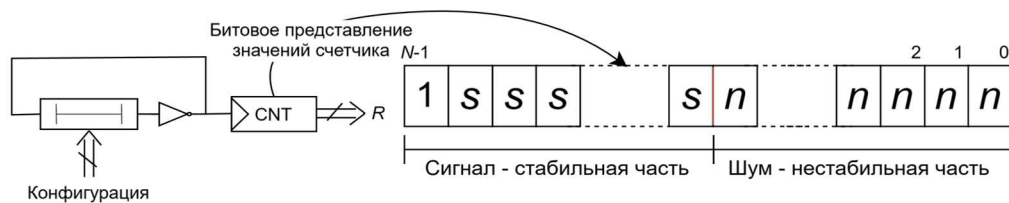


Рисунок 1 – Схема ФНФ КО и получаемые значения

Пусть $M_{\text{фнф}} = \{R_0, R_1, R_2, \dots, R_{m-1}\}$, опытным путем было выяснено, что при переводе значений R_i в бинарный вид, каждый разряд $R_i^j \in \{0, 1\}$, $j \in [0, N-1]$, где $N = \lceil \log_2(\max(M_{\text{фнф}})) \rceil$, будет иметь определенную вероятность искажения p_j на наборе из m элементов:

$$p_j = \max\{p_{j0}, p_{j1}\}, \quad (1)$$

$$\text{где } p_{j0} = \frac{1}{m} \sum_{i=0}^{m-1} R_i^j, \quad p_{j1} = 1 - p_{j0}.$$

Как было установлено экспериментальным путем, значения R_i представляют собой статистические шаблоны. R_i^j можно условно поделить на три группы $A(p_j = 1)$, $B(0,5 + \varepsilon < p_j < 1)$, где $\varepsilon < 0,01$, и $C(p_j = 0,5 + \varepsilon)$, размерами соответственно a, b, c , где $a + b + c = N$, $R_i = [A_i, B_i, C_i]$. По мажоритарному принципу группы B можно привести к группе A .

Была выдвинута гипотеза, что при достаточно больших m множество $M_{\text{фнф}}$ будет образовывать дискретное нормальное распределение. Для подтверждения данной гипотезы была построена программная математическая модель схемы ФНФ КО со счетчиком на базе библиотеки numpy языка Python, которая генерирует дискретную выборку $M_{\text{мод}}$ заданного размера с фиксированными значениями математического ожидания μ и дисперсии σ^2 . При сравнении p_j между счетчиком и математической моделью, была получена погрешность $\gamma < 0,001$, что говорит о схожести полученных значений счетчика с нормальным распределением.

Была сформирована гипотеза об оценке размерности нестабильной группы C , которая основана на разнице значений $\min$ и $\max$:

$$c_{теор_1} = \lceil \log_2(\max(M_{мод}) - \min(M_{мод})) \rceil. \quad (2)$$

Несмотря на сходство между теоретическими и экспериментальными P_j , $\max(M_{мод}) - \min(M_{мод}) < \max(M_{фнф}) - \min(M_{фнф})$, поэтому данная характеристика для значений ФНФ будет менее точной, чем на основании σ .

В теоретическом нормальном распределении 99,7% значений принадлежат диапазону $(-3\sigma; 3\sigma)$

[3]. Была выдвинута другая гипотеза, что шум можно оценить значением $c_{теор_2}$, основываясь на среднеквадратичном отклонении:

$$c_{теор_2} = \lceil \log_2(6\sigma) \rceil. \quad (3)$$

При проведении различных экспериментов с заданными μ и σ^2 , было показано, что $c < c_{теор_2} < c_{теор_1}$.

Тем самым, можно оценить размер стабильной части значением $(a+b)_{теор}$. И, как следствие, количество бит $(a+b)_{теор}$ можно считать уникальным идентификатором, который длиннее, чем a :

$$a+b > (a+b)_{теор} = N - \lceil \log_2(6\sigma) \rceil > a. \quad (4)$$

Параметры μ и σ^2 влияют на размерности a, b, c . Для исследования границ группы $p_j = 0,5 + \varepsilon$, было взято $\mu' = 2^{K+1} + 2^K$, $1 < 3\sigma' < 2^{K-2}$, где $\mu', \sigma', K \in \mathbb{Z}$. В таком случае, $p_{K-1} = 1$, $p_k = 0,5$, $k \in [0, K-2]$. Это объясняется симметричностью нормального распределения.

Для приведения группы $B_{мод}$ к сильно нестабильной части, необходимо $\mu_{мод} = [A_{мод}, B_{мод}, C_{мод}] \in \mathbb{R}^3$ преобразовать в значение $\mu^* = [A_{мод}, [10...0]_{b_{мод}}, [0...0]_{c_{мод}}] \in \mathbb{R}^3$. Для этого, от каждого $R_i \in M_{мод}$ необходимо вычесть $\Delta = \mu_{мод} - \mu^*$. Тем самым будут получены $b+c$ равномерно распределенных разрядов. Как показано на рисунке 2, слева – отображены значения p_{j1} , справа – p_j .

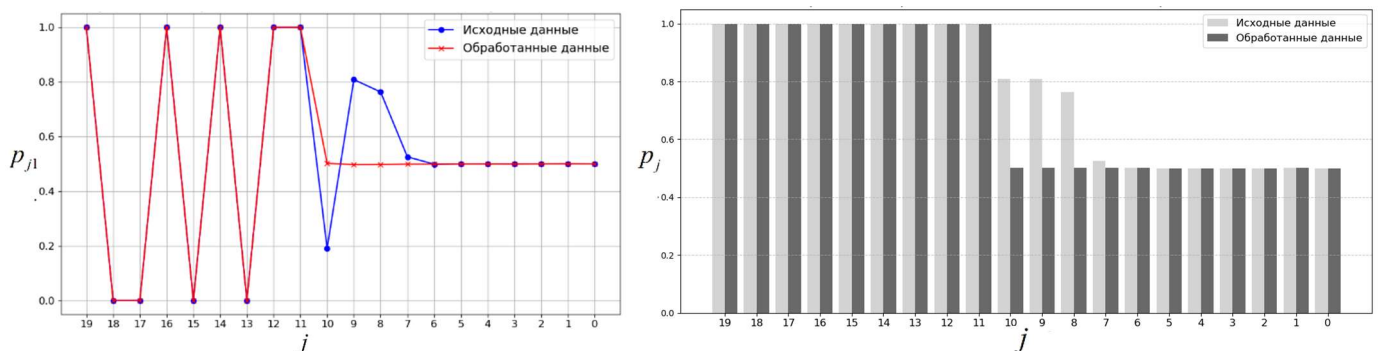


Рисунок 2 – Преобразование распределения

В результате, в зависимости от имеющейся задачи, можно получить как источник случайных чисел с $b+c$ равномерно распределенными каналами, так и уникальный идентификатор с длиной больше, чем полная стабильная группа A . Для обеспечения большей случайности к сильно нестабильной части можно применить различные алгоритмы и методы постобработки. Данное исследование показывает, что

природа ФНФ КО действительно случайна, и значения счетчика, изменяемые из-за случайных шумов во время работы КО, образуют нормальное распределение.

Список использованных источников:

1. Иванюк, А. А. Применение конфигурируемых генераторов импульсов для идентификации ПЛИС / А. А. Иванюк // Информатика. №4(32), 2011. – С. 113–123.
2. Бурко, Л. А. Исследование поведения кольцевого осциллятора / Л. А. Бурко, А. А. Иванюк // Информационные технологии и системы 2024 (ИТС 2024) = Information Technologies and Systems 2024 (ITS 2024) : материалы международной научной конференции, Минск, 20 ноября 2024 г. / Белорусский государственный университет информатики и радиоэлектроники ; редкол. : Л. Ю. Шилин [и др.]. – Минск, 2024. – С. 81–82.
3. Справочник по теории вероятностей и математической статистике / Корольков В. С. [и др.]. – Москва : Наука, 1985. – 640 с.