УДК: 004.312

# СТАТИСТИЧЕСКОЕ ИССЛЕДОВАНИЕ ДАННЫХ, ПОЛУЧЕННЫХ С ФНФ НА КОНФИГУРИРУЕМЫХ КОЛЬЦЕВЫХ ОСЦИЛЛЯТОРАХ

*Бурко Л.А., магистрант*

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

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

**Аннотация.** В работе исследуется распределение значений физически неклонируемой функции на основе конфигурируемых кольцевых осцилляторов. Для проверки гипотезы о нормальности распределения использованы гистограммы, QQ-графики и статистические тесты Шапиро-Уилка, Д'Агостино-Пирсона, Жарка-Бера и Андерсона-Дарлинга (scipy.stats).

**Ключевые слова.** Физическая криптография, физически неклонируемые функции, конфигурируемый кольцевой осциллятор, генерация случайных данных, тесты на нормальность.

В современных цифровых системах случайные числа применяются повсеместно. Они играют ключевую роль в обеспечении безопасности, точности и надежности вычислительных процессов. Поэтому вопросы, связанные с эффективной генерацией случайных чисел, остаются актуальным предметом многих научных исследований. Помимо этого, находят применение в криптографии и нормально распределенные данные. Например, алгоритмы типа Kyber или Dilithium используют дискретное нормальное распределение для добавления «малого» шума к секретным данным. Это делает задачу нахождения закрытого ключа вычислительно неразрешимой, так как шум маскирует структуру решетки (решеточная криптография). Нормальное распределение можно также использовать для моделирования физических процессов в криптографии и в дифференциальном анализе, который используется при тестировании криптостойкости, когда необходимо смоделировать распределение ошибок или вероятностей при попытке взлома системы.

Физически неклонируемые функции (ФНФ), реализуемые на базе программируемых логических интегральных схем, находят широкое применение в задачах аппаратной безопасности и генерации случайных чисел благодаря сочетанию уникальных физических свойств и гибкости реконфигурируемой логики. Физически неклонируемая функция – это функция, которая использует физические особенности конкретного устройства для генерации уникального и неклонируемого ответа на основе запроса. Основой функционирования ФНФ являются неконтролируемые технологические вариации, возникающие в процессе изготовления интегральных схем и обусловленные физическими свойствами полупроводниковых элементов. Распространённым примером является ФНФ на кольцевых осцилляторах (КО ФНФ), в которой отклик формируется на основе сравнений частот нескольких идентичных кольцевых осцилляторов. Конфигурируемый кольцевой осциллятор (ККО) позволяет получать множество частотных состояний за счёт выбора различных внутренних конфигураций при фиксированном числе генераторов. Данная архитектура, описанная подробно в [1, 2], формирует многобитный ответ. На точность измерения периода сигнала ККО будет влиять ширина окна измерения (множитель периода сигнала системной частоты $k_{factor} = 2^i, i \in \mathbb{Z}$).

На рисунке 1 показана схема работы ФНФ. Пара, состоящая из входного параметра запроса (Challenge) и соответствующего ему выходного параметра ответа (Responce), называется парой «запрос–ответ».

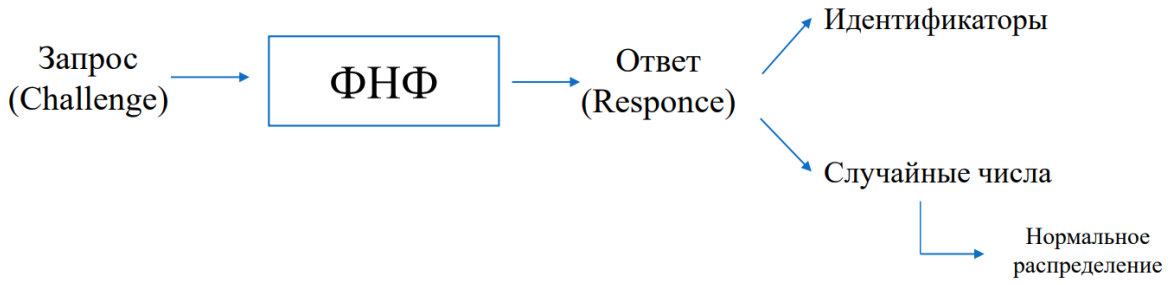


Рисунок 1 – Упрощенная схема ФНФ

Процесс эксперимента начинается с этапа описания архитектуры ФНФ и её аппаратной реализации в среде Vivado, где выполняются синтез, размещение, трассировка и формирование битового файла для программирования платы. Далее конфигурация загружается на отладочную платформу, где

осуществляется непосредственная аппаратная реализация ФНФ и генерация откликов. Параллельно в среде Xilinx Vitis разрабатывается программная часть, отвечающая за формирование запросов, управление режимами работы и передачу данных. Обмен информацией между платой и персональным компьютером осуществляется через терминальную программу TeraTerm, обеспечивающую чтение и запись данных по последовательному интерфейсу. Полученные значения ФНФ передаются в среду анализа на базе Python (Jupyter Notebook с использованием библиотек NumPy, pandas и matplotlib), где выполняется их статистическая обработка, оценка стабильности, уникальности и построение соответствующих графиков. Схема на рисунке 2 отражает полный цикл – от аппаратного проектирования ФНФ до программного анализа экспериментальных результатов.

Эксперимент проводился на плате быстрого прототипирования Digilent ZYBO-Z7 (кристалл Xilinx ZYNQ xc7z010-1).

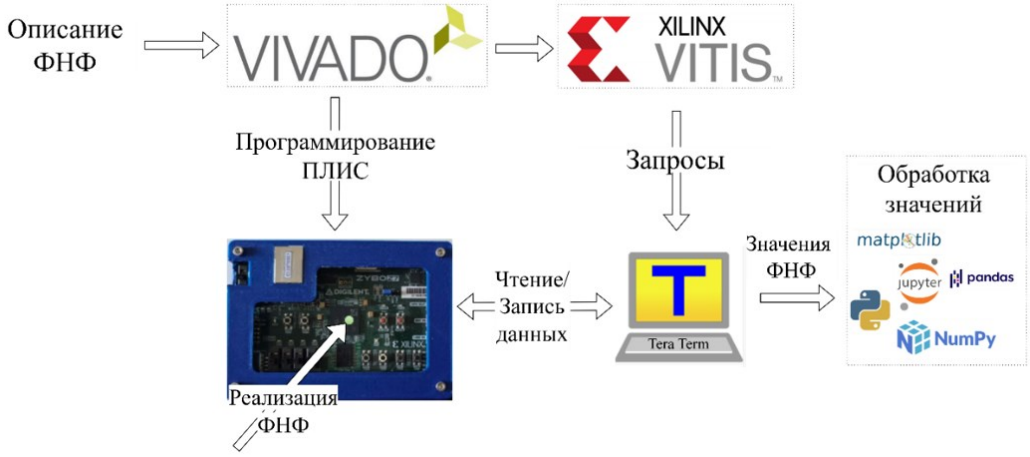


Рисунок 2 – Схема эксперимента

Был получен 31 набор данных с параметром $i \in [0; 30]$, каждый из которых содержит $M = 1000$ целочисленных значений.

При построении гистограмм распределения значений с ФНФ ККО, начиная с $i = 9$, наблюдается сходство с нормальным распределением. В работе [1] уже была показана высокая степень сходства поразрядных вероятностей данных ФНФ ККО с нормальным распределением, а также был определен оптимальный диапазон для окна измерения $i \in [9; 30]$. Также было показано, что разряды можно разделить на три группы: сильно стабильные (вероятность появления определенного бита 100%), сильно нестабильные (вероятность появления определенного бита 50%) и слабо стабильные (вероятность появление определенного бита от 50% до 100%).

Как видно на рисунке 3, дальнейшее исследование для $i<15$ нецелесообразно, поскольку уменьшение $i$ приведёт лишь к ухудшению согласия с нормальным распределением из-за большей дискретности и возможной асимметрии, не давая при этом качественно новой информации о поведении выборки.

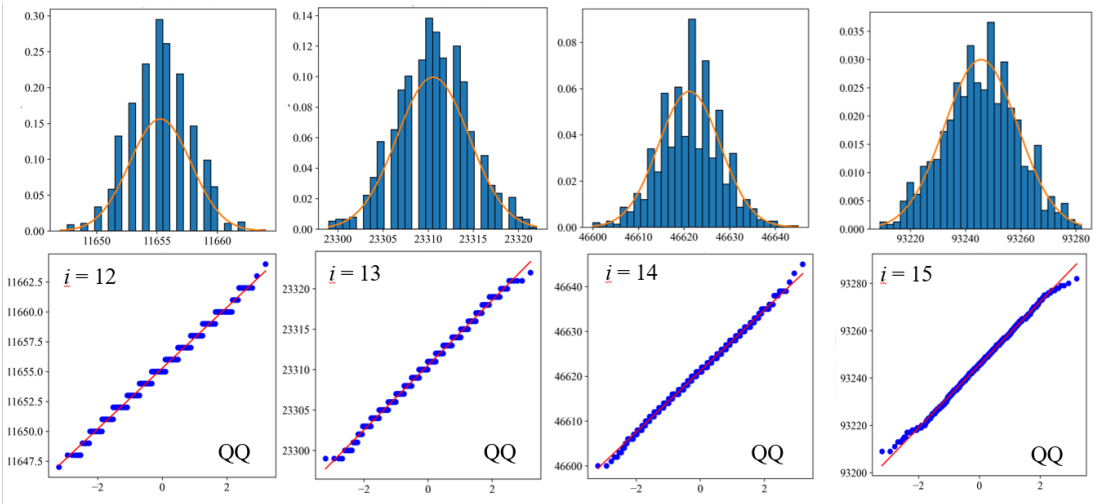


Рисунок 3 – QQ-тест и кривая нормального распределения для $i = \{12,13,14,15\}$

Целью данного исследования является анализ данных, полученных с ФНФ ККО, относительно нормального распределения для выбора наиболее подходящих *i* для дальнейших задач идентификации или генерации случайных чисел. Для этого был применён комплекс графических и статистических методов, позволяющих как качественно, так и количественно оценить степень соответствия экспериментальных данных нормальному распределению.

К графическим методам относятся гистограммы распределения и QQ-графики, примеры для *i* = {19, 23, 25, 26} показаны на рисунке 4. Гистограмма позволяет визуально оценить форму распределения и сравнить её с теоретической плотностью нормального распределения. Для этого на гистограмму накладывается соответствующая нормальная кривая, параметры (МО и СКО) которой оцениваются по выборке.

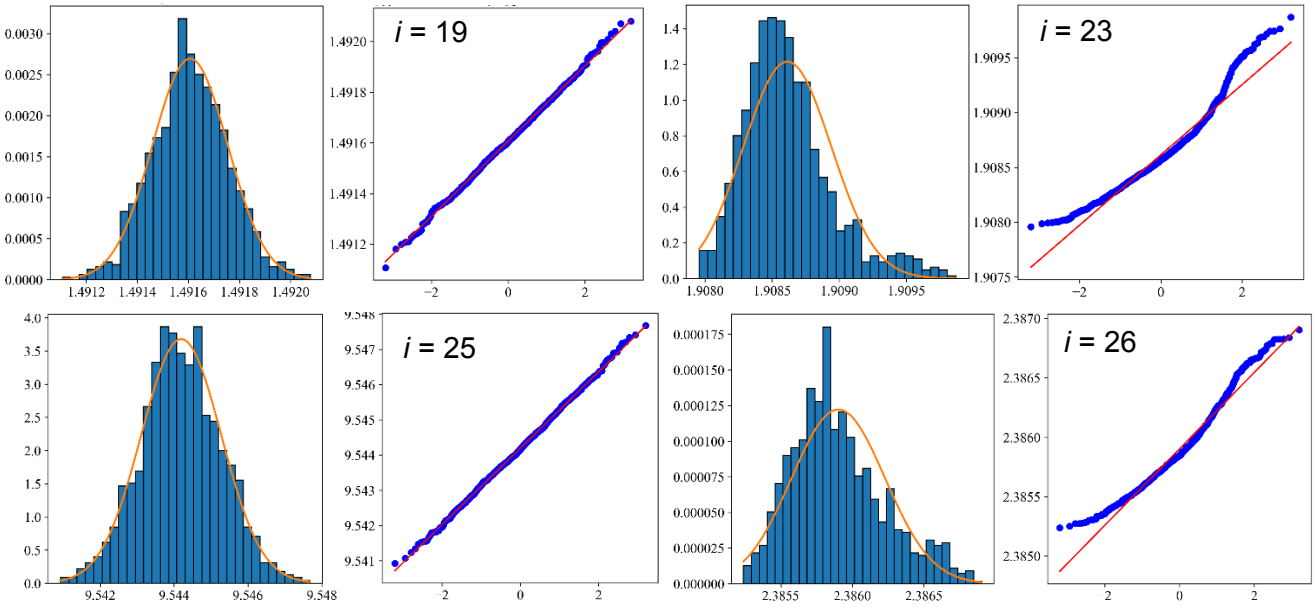


Рисунок 4 – QQ-тест и кривая нормального распределения для *i* = {19, 23, 25, 26}

Более информативным инструментом является QQ-график (quantile-quantile plot), на котором откладываются квантили экспериментальных данных относительно квантилей теоретического нормального распределения. В случае соответствия распределения нормальному закону точки на графике располагаются вдоль прямой линии. Отклонения от линейности свидетельствуют о несоответствии распределения нормальному закону, при этом характер отклонений позволяет выявить особенности распределения. Так, отклонения в центральной части указывают на изменение формы распределения, а отклонения на концах – на различия в поведении хвостов (наличие выбросов или тяжёлых хвостов).

На рисунке 4 QQ-график показывает хорошее совпадение в центральной части распределения, при этом наблюдаются отклонения в хвостах для *i* = 23 и *i* = 26, что свидетельствует о наличии более тяжёлых хвостов по сравнению с нормальным распределением. Это пример сильного отклонения от нормального распределения, в случаях *i* = 19 и *i* = 25 не наблюдается отклонений в хвостах.

Для количественной проверки гипотезы нормальности было использовано несколько статистических критериев: тест Шапиро-Уилка (stats.shapiro), тест Д'Агостино-Пирсона (stats.normaltest), критерий Жарка-Бера (stats.jarque_bera) и критерий Андерсона-Дарлинга (stats.anderson). Применение нескольких тестов обусловлено различной чувствительностью каждого из них к отдельным характеристикам распределения.

Тест Шапиро-Уилка является одним из наиболее мощных критериев проверки нормальности, особенно для выборок малого и среднего размера. Он основан на сравнении упорядоченных значений выборки с ожидаемыми значениями нормального распределения. В качестве результата вычисляется статистика теста и значение p-value. Если p-value превышает заданный уровень значимости (обычно 0,05), то нет оснований отвергать гипотезу нормальности.

Тест Д'Агостино-Пирсона основан на анализе двух характеристик распределения: асимметрии и эксцесса. Он объединяет их в единую статистику, позволяющую оценить отклонение распределения от нормального. Тест чувствителен к асимметрии распределения и отклонениям в форме хвостов. Интерпретация результата аналогична тесту Шапиро-Уилка и осуществляется по значению p-value.

Критерий Жарка-Бера также основан на анализе асимметрии и эксцесса распределения. Нулевая гипотеза заключается в том, что асимметрия равна нулю и эксцесс соответствует

нормальному распределению. Отклонение хотя бы одной из этих характеристик приводит к отклонению гипотезы нормальности.

Критерий Андерсона-Дарлинга является модификацией критерия согласия, обладающей повышенной чувствительностью к отклонениям в хвостах распределения. В отличие от предыдущих тестов, он не использует p-value, а сравнивает вычисленную статистику с критическими значениями. В рамках проведённого исследования использовались стандартные уровни значимости (15%, 10%, 5%, 2,5% и 1%). Полученные значения статистики критерия интерпретировались следующим образом: значения менее 0,5 свидетельствуют о высокой степени согласия эмпирического распределения с нормальным законом; диапазон 0,5-0,8 также рассматривается как допустимый и не указывает на существенные отклонения. При увеличении значения статистики наблюдается рост степени расхождения распределения с нормальным, что указывает на ухудшение соответствия рассматриваемой модели.

Как показано в таблице 1, для $i$ = {15, 17, 18, 19, 21, 25} все применённые статистические тесты дают высокие значения p-value, что не позволяет отвергнуть гипотезу нормальности. Значения статистики критерия Андерсона–Дарлинга находятся в низком диапазоне, что указывает на хорошее соответствие нормальному закону. Для $i$ = 16 и $i$ = 20 всего лишь один из применённых статистических критериев не выявляет отклонений от нормального распределения. В остальных случаях наблюдаются статистически значимые отклонения от нормальности. Например, при $i$ = 29 значения p-value остаются ненулевыми, но ниже порога 0,05, что также свидетельствует об отклонении.

Тем не менее, как было показано в предыдущих исследованиях [1, 2], применение дополнительных преобразований позволяет получить необходимые характеристики для задач идентификации или генерации случайных чисел.

Таблица 1 – Статистические тесты для $i \in [15; 30]$.

| *i* | Шапиро-Уилка | Д'Агостино-Пирсона | Жарка-Бера | Андерсона- Дарлинга |
|---|---|---|---|---|
| 15 | **0,06783** | **0,11026** | **0,17046** | **0,51364** |
| 16 | 0,04606 | 0,02944 | **0,05439** | 0,97937 |
| 17 | **0,17797** | **0,22958** | **0,27464** | **0,42452** |
| 18 | **0,19346** | **0,30956** | **0,33125** | **0,26324** |
| 19 | **0,88472** | **0,76686** | **0,80928** | **0,24794** |
| 20 | 0,01884 | 0,00458 | 0,00440 | **0,65561** |
| 21 | **0,21644** | **0,19082** | **0,20286** | **0,21787** |
| 22 | 0,00010 | 0,00049 | 0,00040 | 1,80514 |
| 23 | 0,00000 | 0,00000 | 0,00000 | 8,88308 |
| 24 | 0,00032 | 0,00123 | 0,00117 | 1,51951 |
| 25 | **0,91052** | **0,85152** | **0,84501** | **0,26550** |
| 26 | 0,00000 | 0,00000 | 0,00000 | 12,96655 |
| 27 | 0,00000 | 0,00004 | 0,00009 | 4,74584 |
| 28 | 0,00000 | 0,00000 | 0,00000 | 3,16967 |
| 29 | 0,00141 | 0,01610 | 0,01427 | 1,84256 |
| 30 | 0,00002 | 0,00395 | 0,00496 | 3,00161 |

В рамках данной работы было проведено комплексное статистическое исследование данных, полученных с физически неклонируемой функции на основе конфигурируемых кольцевых осцилляторов. Основной целью являлась проверка гипотезы о нормальности распределения значений ФНФ при различных параметрах окна измерения $i$, а также определение диапазона параметров, наиболее подходящих для практического применения в задачах идентификации и генерации случайных чисел.

Проведённый анализ включал как графические методы (гистограммы и QQ-графики), так и количественные критерии (тесты Шапиро-Уилка, Д'Агостино-Пирсона, Жарка-Бера и Андерсона-Дарлинга). Это позволило получить всестороннюю оценку распределений, учитывающую как форму, так и статистические характеристики выборок. Показано, что при малых значениях параметра i наблюдаются существенные отклонения от нормального распределения, обусловленные дискретностью данных и влиянием аппаратных особенностей измерений. Некоторые конфигурации удовлетворяют статистическим характеристикам нормального распределения, и в них группа слабо нестабильных бит меньше, чем в тех, где распределение не соответствует нормальному. Таким образом, ряд приведенных проверок позволяет выбрать необходимое $i$ в зависимости от требуемой задачи.

***Список использованных источников:***

*1. Иванюк, А.А. Генерирование детерминированных идентификаторов и случайных чисел на основе схемы конфигурируемого кольцевого осциллятора / А.А. Иванюк, Л.А. Бурко // Информатика. 2025, 22(4). – С.65-81. https://doi.org/10.37661/1816-0301-2025-22-4-65-81*

*2. Ivaniuk, A. Unclonable Identification and True Random Number Generation Based on CRO PUF / A. Ivaniuk, L. Burko // Pattern Recognition and Information Processing (PRIP2025): Proceedings of the 17th International Conference, September 16-18, 2025, Minsk, Belarus / UIIP NASB. – Minsk, 2025.– pp. 103-107.*

UDC: 004.312

# STATISTICAL RESEARCH OF DATA FROM PUF BASED ON CONFIGURABLE RING OSCILLATORS

*Burko L.A., master's student*

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

*Ivaniuk A.A. – PhD in Technical Sciences*

**Annotation.** This research examines the distribution of values of a physically unclonable function based on configurable ring oscillators. Histograms, QQ-plots, and the Shapiro-Wilk, D'Agostino-Pearson, Jarque-Bera, and Anderson-Darling statistical tests (from scipy.stats) were used to test the hypothesis of normality.

**Keywords.** physical cryptography, physically unclonable functions, configurable ring oscillator, random numbers generation, normality tests.