

Исследование поведения бистабильных элементов, реализованных на ПЛИС

Кайки Михаил Николаевич, м.т.н.

- аспирант специальности 05.13.05 «Элементы и устройства вычислительной техники и систем управления», БГУИР
- ассистент кафедры программного обеспечения информационных технологий, БГУИР

Иванюк Александр Александрович, д.т.н., профессор

- профессор кафедры информатики, БГУИР

Актуальность

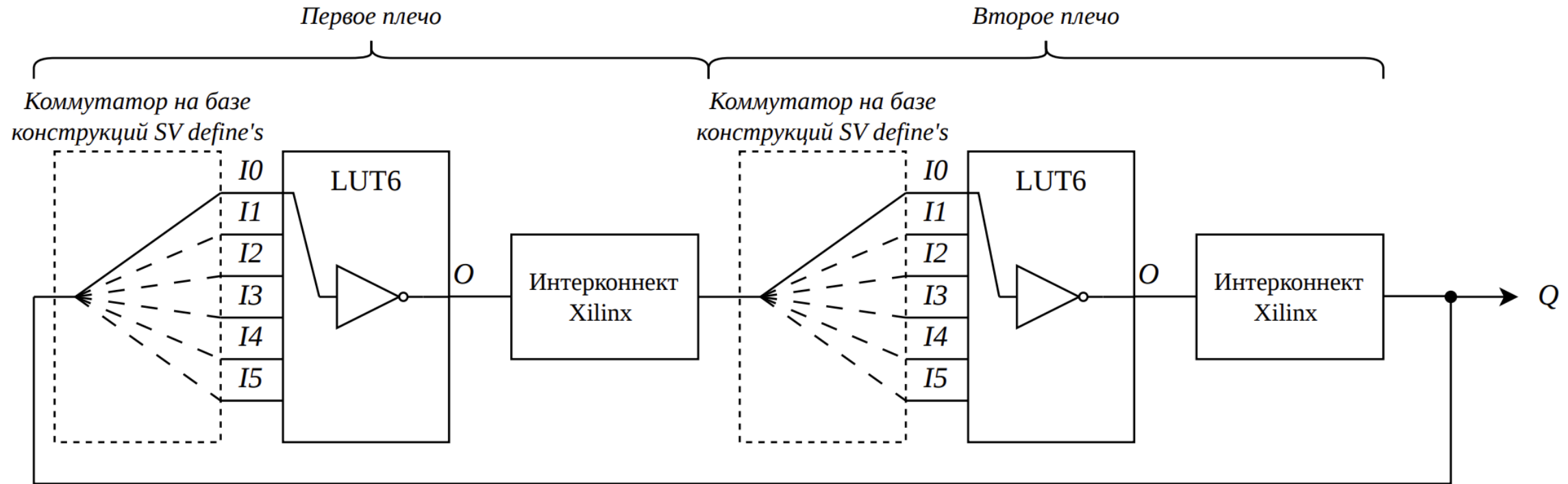
Физически неклонлируемые функции – это функции, воплощённые в физической структуре, которые просто оценить, но трудно охарактеризовать, смоделировать или воспроизвести.

Бистабильные элементы, такие как RS-защёлки, относятся к классу ФНФ на базе памяти и являются сильными ФНФ по классификации мощности множества пар «запрос – ответ».

Где востребованы ФНФ на ПЛИС:

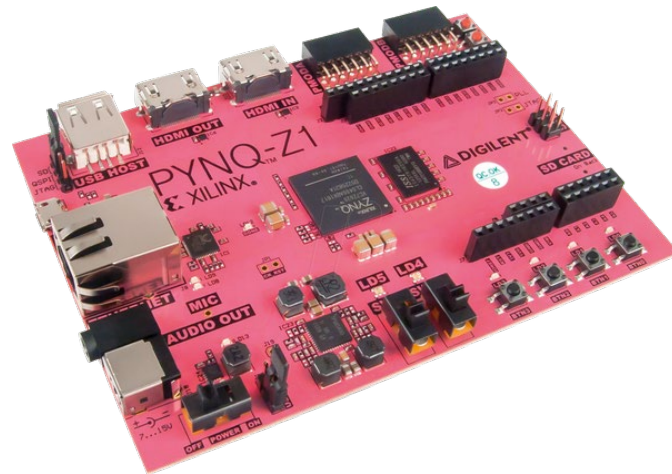
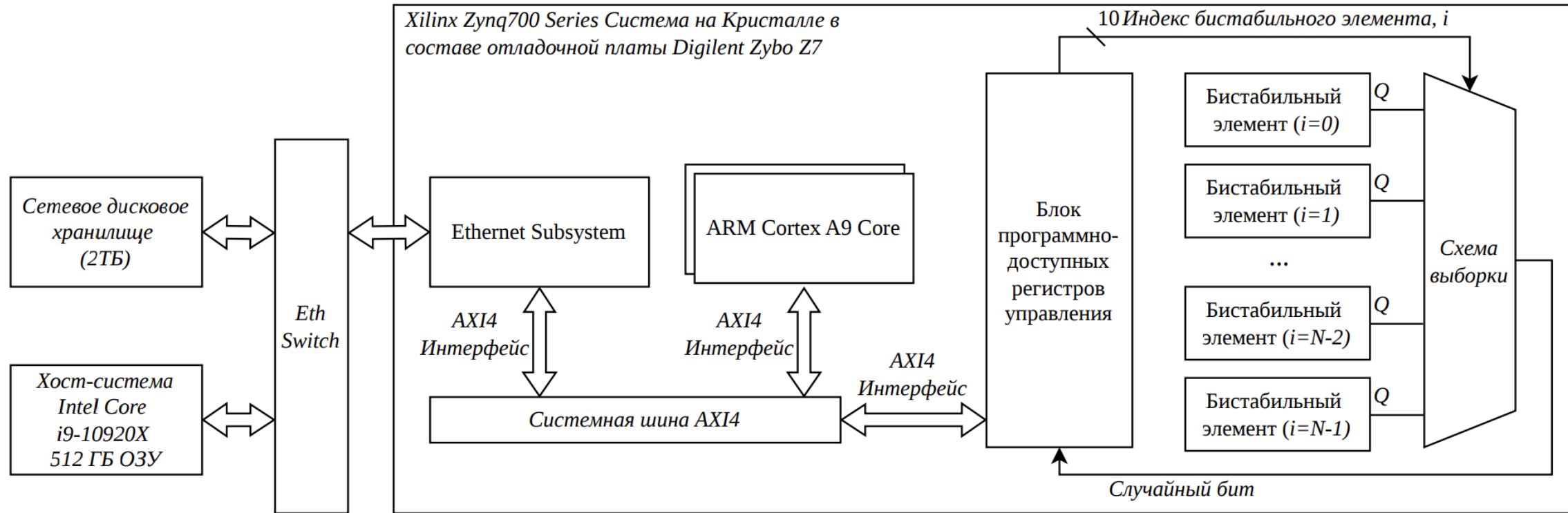
- Криптографическая защита информации: генерация ключей, начальных векторов, сессионных токенов.
- Встраиваемые и промышленные системы, где нет отдельных аппаратных ГСЧ, а ПЛИС уже присутствует в составе устройства.
- Аппаратная аутентификация и идентификация устройств, защита от клонирования

Бистабильные элементы, реализованные на базе ПЛИС



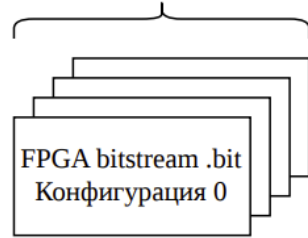
Для исследования влияния сетей маршрутизации в экземплярах ПЛИС на качество генерируемых последовательностей начальных состояний элементов были сформированы все возможные 36 конфигураций обратных связей при помощи конструкции *define* препроцессора языка описания аппаратуры SystemVerilog. Для ограничения работы синтезатора также были подготовлены 36 файлов с указанием местоположения каждого из $2 \cdot N = 2048$ элементов LUT6 на кристалле ПЛИС.

Программно – аппаратный комплекс для проведения эксперимента

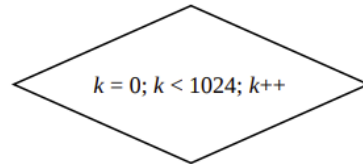
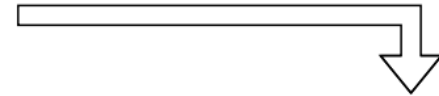


Ход эксперимента

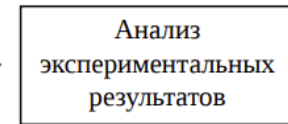
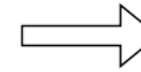
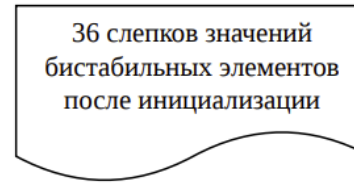
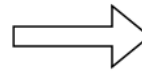
36 конфигураций обратных связей
бистабильных элементов



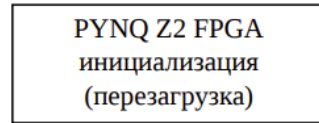
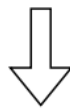
Цикл повторения
процесса инициализации
(перезагрузки) платы



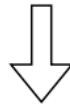
No



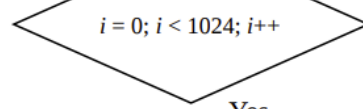
Yes



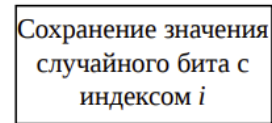
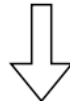
Yes



No



Yes



Цикл чтения значений
инициализации каждого
бистабильного элемента



Анализ полученных данных

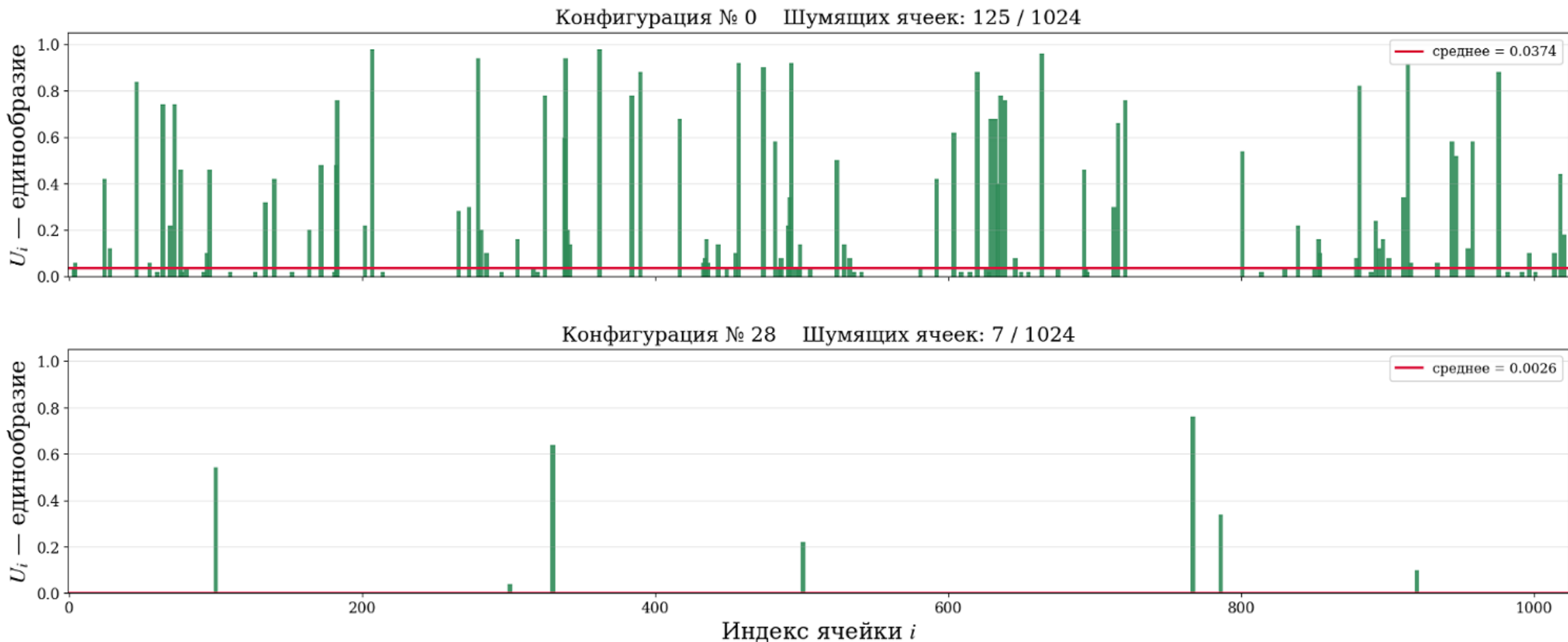
Для анализа полученных данных используем метрику единообразия, которая отображает степень равномерности распределения нулевых и единичных состояний в полученном векторе инициализаций для каждой из ячеек:

$$U_i = 1 - 2 \times \left| \frac{WH(V_i)}{K} - 0,5 \right|,$$

где K – количество циклов перезапуска ПЛИС, V_i – вектор инициализационных значений для ячейки бистабильного элемента с индексом i , $WH(V_i)$ – вес Хэмминга вектора V_i .

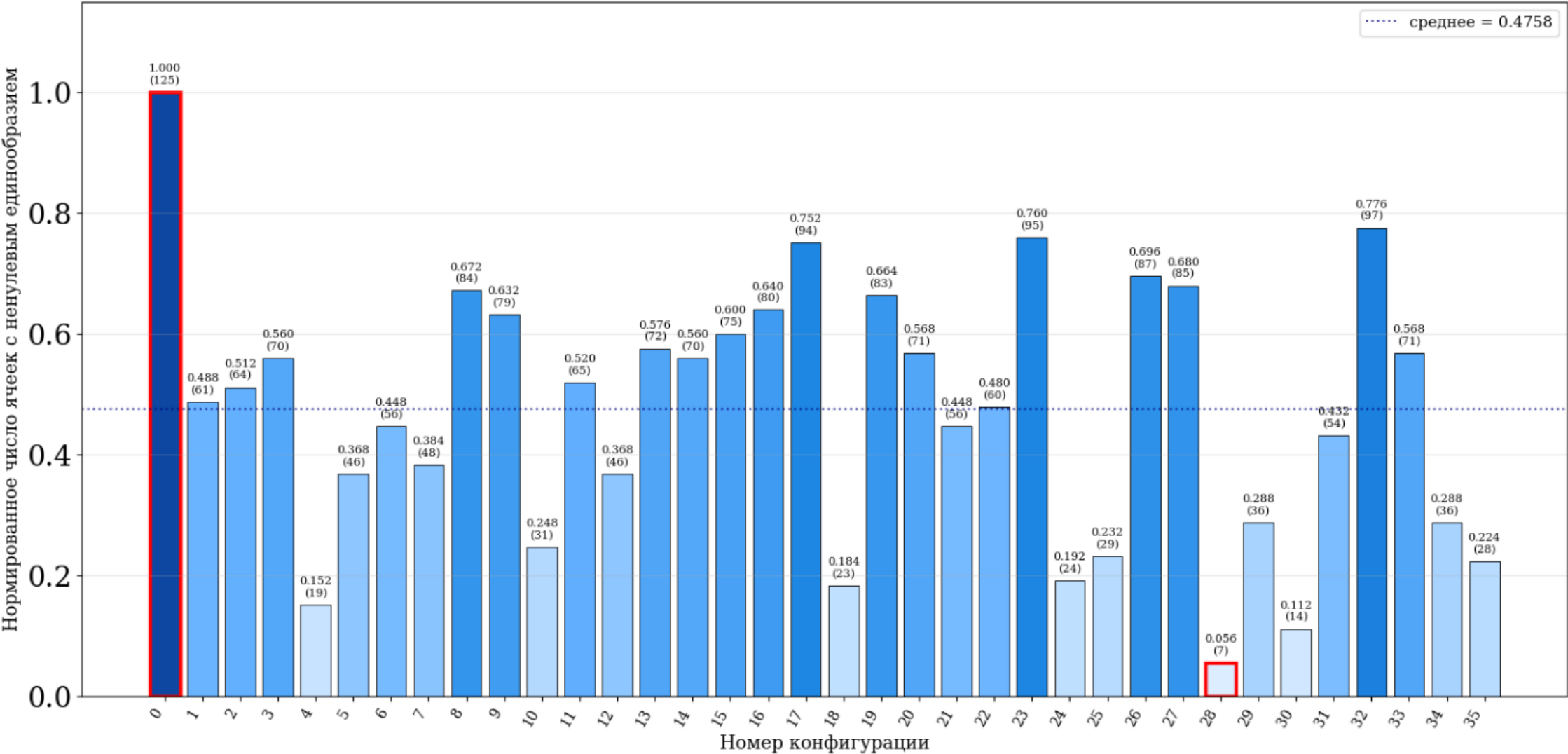
Метрика единообразия принимает значения в диапазоне $[0;1]$: значение $U_i = 1$ соответствует идеально сбалансированному элементу, для которой вероятность единичного состояния $P(1) = 0,5$, а значение $U_i = 0$ – полностью детерминированному элементу, у которого $P(1) = 0$ или $P(1) = 1$ при всех K перезагрузок. Бистабильный элемент будем называть шумящим, если выполняется неравенство $0 < WH(V_i) < K$. Для таких элементов метрика единообразия строго положительна: $U_i > 0$. Элементы, у которых $WH(V_i) = 0$ или $WH(V_i) = K$, будем называть детерминированными: их начальное состояние воспроизводится от перезапуска к перезапуску без изменений, а $U_i = 0$.

Анализ полученных данных



Анализ полученных данных

Диаграмма распределения шумящих ячеек по номеру конфигурации



Заключение

Видно, что распределение конфигураций по числу шумящих ячеек крайне неравномерно: наряду с конфигурациями, дающими 50 – 100 активных ячеек, присутствуют конфигурации с единичными шумящими ячейками (например, № 4 с 12 ячейками, № 25 с 7 ячейками).

Среднее нормированное число ненулевых ячеек составляет 0,476, что указывает на значительную вариативность между конфигурациями. Полученные данные показывают, что выбор пары активных входов LUT6 существенно влияет на итоговый уровень случайности при инициализации ПЛИС.

В работе исследовано влияние сети межсоединений бистабильных элементов на базе LUT6 в ПЛИС на качество генерируемых случайных последовательностей их начальных состояний.

На аппаратной платформе из 1024 бистабильных элементов с 36 возможными вариантами подключения цепей обратной связи выполнена серия экспериментов с многократными перезапусками программируемой логики.

Полученные результаты формируют экспериментальную основу для последующего проектирования ячеек с управляемой степенью рассогласования плеч обратной связи и создания на их основе источников энтропии на базе физически неклонируемых функций в ПЛИС.

Благодарность

Авторы выражают искреннюю благодарность резиденту ПВТ компании «Инженерный Центр Ядро», которая является одним из центров разработки YADRO, за предоставленное оборудование для проведения экспериментов в рамках работы совместной учебной лаборатории с Белорусским государственным университетом информатики и радиоэлектроники.

