



Министерство образования Республики Беларусь

EDA
Conference

Компьютерное
проектирование
в электронике

Белорусский государственный университет информатики и радиоэлектроники

Q-БИТНАЯ ФИЗИЧЕСКИ НЕКЛОНИРУЕМАЯ ФУНКЦИЯ ТИПА КОНФИГУРИРУЕМЫЙ КОЛЬЦЕВОЙ ОСЦИЛЛЯТОР И ОЦЕНКА ЕЕ ХАРАКТЕРИСТИК

Докладчик:

Бурко Лиана Александровна

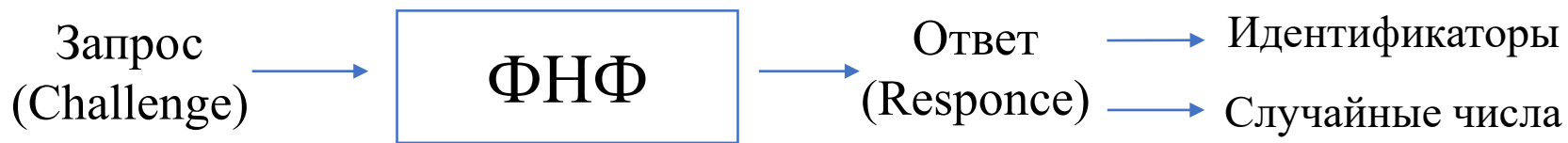
Руководитель:

докт. техн. наук, проф. Иванюк А.А.

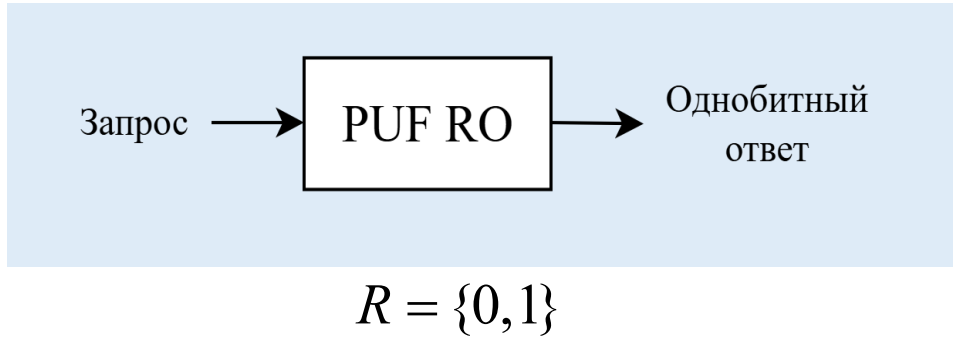
Минск 2026

Актуальность

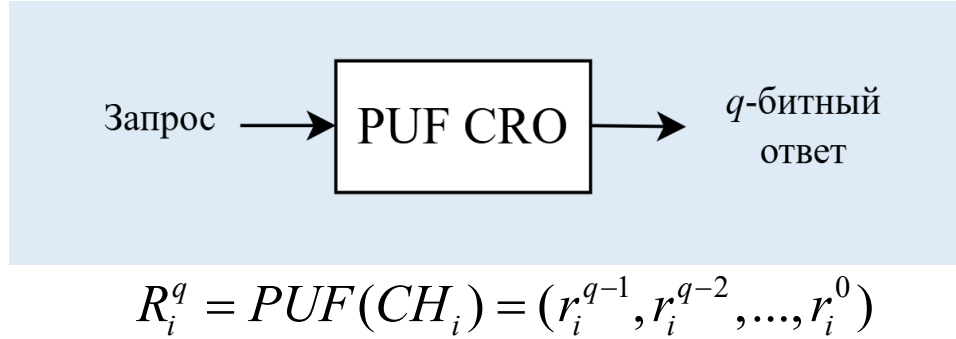
Физически неклонируемая функция – это функция, которая использует физические особенности конкретного устройства для генерации уникального и неклонируемого ответа на основе запроса.



Классическая ФНФ:



Q-битная ФНФ:

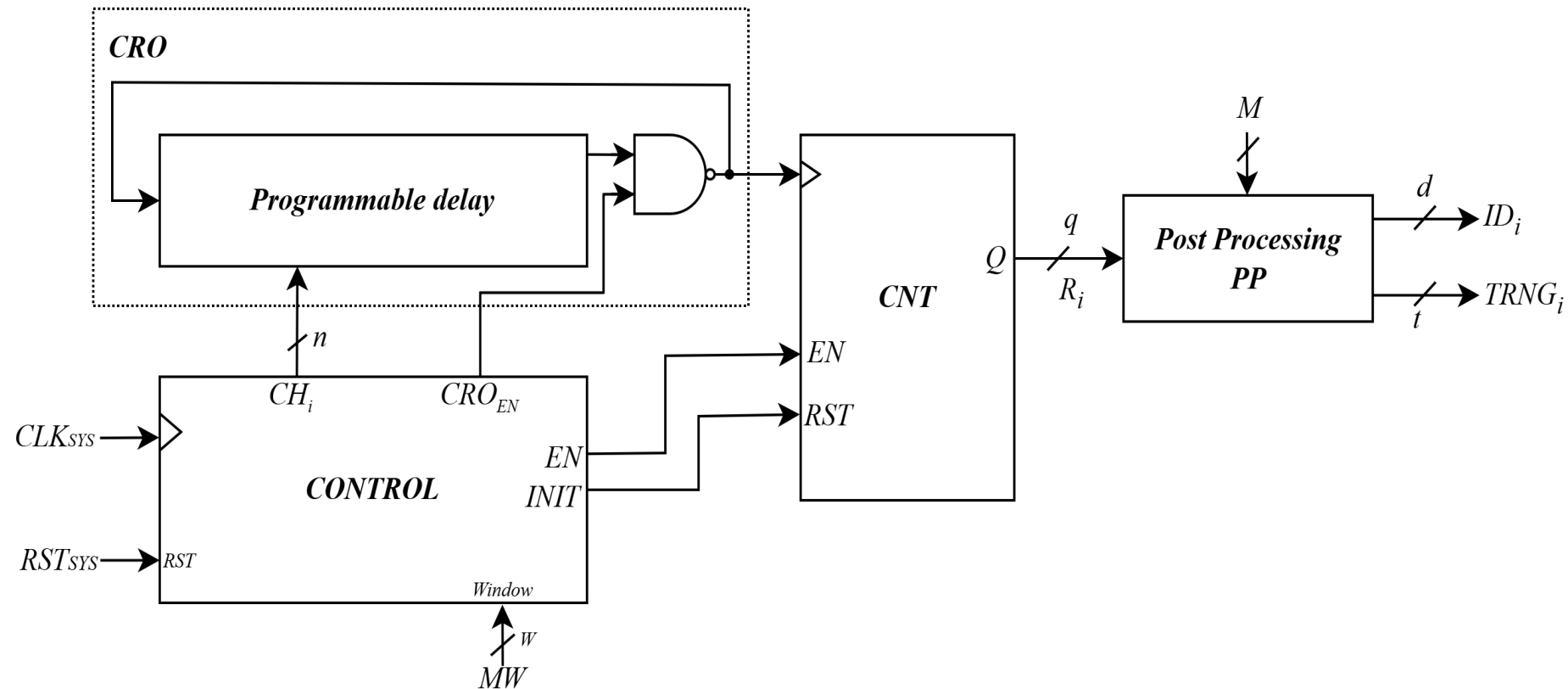


Основные характеристики:

- Стабильность
- Уникальность
- Единообразие

* 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>

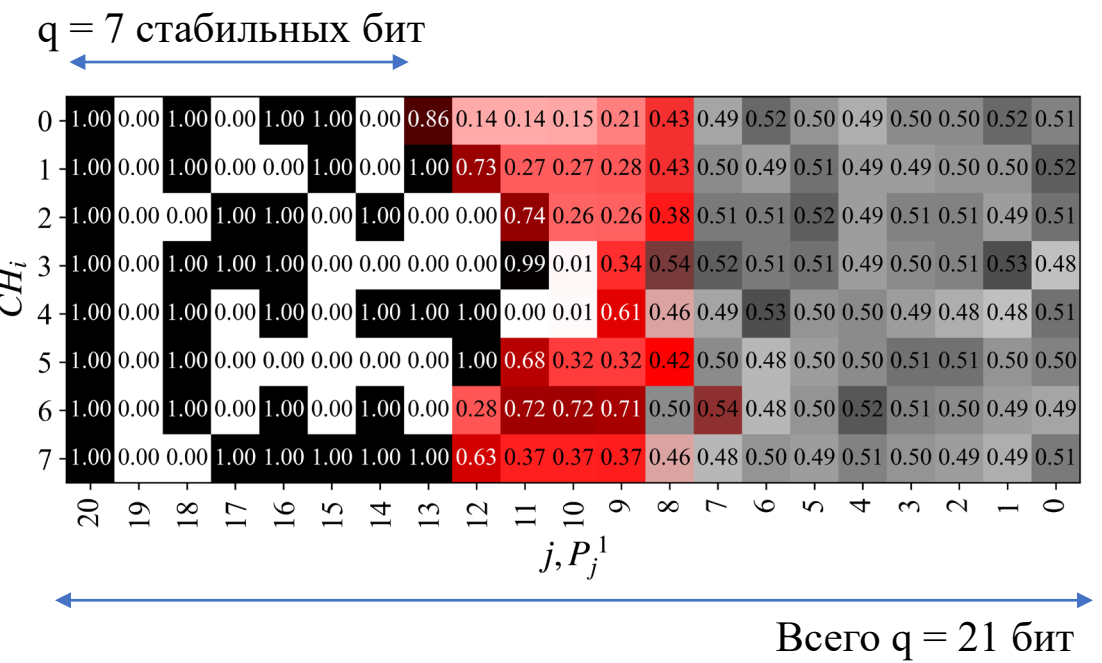
Структурная схема измерения сигналов ККО



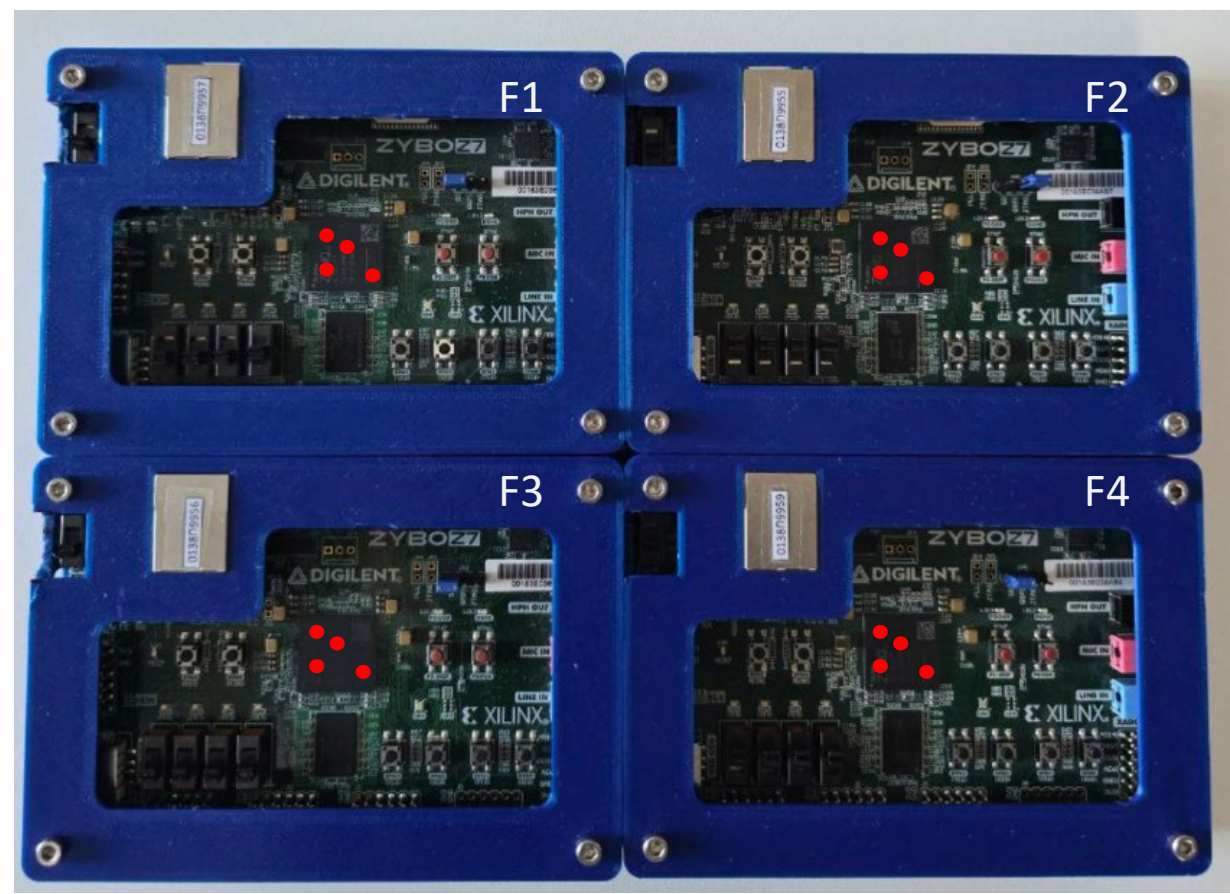
Инструменты для эксперимента:



Экспериментальные результаты проиллюстрированы с помощью наборов данных, полученных для четырех однотипных ПЛИС, содержащих четыре идентичные ФНФ схемы на основе ККО.



Fast Prototyping Board: Digilent ZYBO Z7-10
FPGA: Xilinx ZYNQ 7000



C_0 C_1
 C_2 C_3

- четыре одинаковых ФНФ ККО

Стабильность характеризует способность ФНФ ККО воспроизводить один и тот же ответ при многократных запросах в рамках одной конфигурации.

Для однобитного:

$$p(R_i = 1) = \frac{1}{M} \sum_{j=0}^{M-1} R_i$$

$$Stability_1(R_i) = \max(p(R_i = 1), 1 - p(R_i = 1))$$

Для многобитного:

$$p(r_i^l = 1) = \frac{1}{M} \sum_{j=0}^{M-1} r_i^l$$

$$Stab(r_i^l) = \max(p(r_i^l = 1), 1 - p(r_i^l = 1))$$

$$Stability_q(R_i^q) = \frac{1}{q} \sum_{l=0}^{q-1} Stab(r_i^l)$$

$$\overline{Stability_q} = \frac{1}{T} \sum_{i=0}^{T-1} Stability_q(R_i^q)$$

	ККО ₁		ККО ₂		ККО ₃		ККО ₄	
	$\overline{Stability_{21}}$	$\overline{Stability_7}$	$\overline{Stability_{21}}$	$\overline{Stability_7}$	$\overline{Stability_{21}}$	$\overline{Stability_7}$	$\overline{Stability_{21}}$	$\overline{Stability_7}$
ПЛИС ₁	0,761	0,996	0,760	0,995	0,761	0,997	0,762	0,997
ПЛИС ₂	0,763	0,996	0,765	0,998	0,762	0,996	0,765	0,997
ПЛИС ₃	0,762	0,997	0,761	0,997	0,761	0,996	0,763	0,997
ПЛИС ₄	0,761	0,997	0,760	0,996	0,760	0,996	0,760	0,996

Стабильность

Высокая средняя побитовая стабильность не гарантирует полного совпадения всего q -битного ответа при каждом измерении. Поэтому для оценки возможности непосредственного воспроизведения ответов дополнительно может использоваться **вероятность полного совпадения ответа**.

Для многобитного:

$$P_q^{full}(R_i^q) = \frac{N_{full}(R_i^q)}{M}$$

$$\overline{P_q^{full}} = \frac{1}{T} \sum_{i=0}^{T-1} P_q^{full}(R_i^q)$$

где $N_{full}(R_i^q)$ – количество измерений, при которых сформированный q -битный ответ полностью совпал с эталонным ответом (наиболее встречаемым) для данного запроса.

	ККО ₁		ККО ₂		ККО ₃		ККО ₄	
	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$	$\overline{P_{21}^{full}}$	$\overline{P_7^{full}}$
ПЛИС ₁	0,0067	0,9913	0,0067	0,9863	0,0067	0,9912	0,0066	0,9905
ПЛИС ₂	0,0068	0,9869	0,0067	0,9925	0,0067	0,9890	0,0067	0,9894
ПЛИС ₃	0,0067	0,9907	0,0066	0,9899	0,0066	0,9890	0,0065	0,9920
ПЛИС ₄	0,0068	0,9914	0,0066	0,9882	0,0065	0,9896	0,0065	0,9872

Уникальность

Уникальность характеризует способность ФНФ ККО формировать уникальные ответы для различных входных воздействий и, соответственно, отсутствие коллизий между ответами на различных экземплярах.

Для однобитного:

однобитные ответы: $R_{a,i}, R_{b,i}$

$$Uniq_1(R_{a,i}, R_{b,i}) = \frac{1}{T} \sum_{i=0}^{T-1} [R_{a,i} \oplus R_{b,i}]$$

Для многобитного:

q -битные ответы: $R_{a,i}^q, R_{b,i}^q$

$$Uniq_q(R_{a,i}^q, R_{b,i}^q) = \frac{1}{T \cdot q} \sum_{i=0}^{T-1} HD[R_{a,i}^q, R_{b,i}^q]$$

Один ККО на всех четырех экземплярах ПЛИС

Межкристальная оценка уникальности:

ККО₁ – 0,482964,

ККО₂ – 0,478217,

ККО₃ – 0,479791,

ККО₄ – 0,482322.

Одна ПЛИС для всех четырех ККО

Внутрикристальная оценка уникальности:

ПЛИС₁ – 0,427734,

ПЛИС₂ – 0,420058,

ПЛИС₃ – 0,419027,

ПЛИС₄ – 0,427544.

Для каждого символа k алфавита выходной последовательности определяется число его появлений на T запросах:

$$C(k) = |\{R_i^q = k\}|,$$

где $k \in \{0, \dots, 2^q - 1\}, i \in [0, T - 1]$

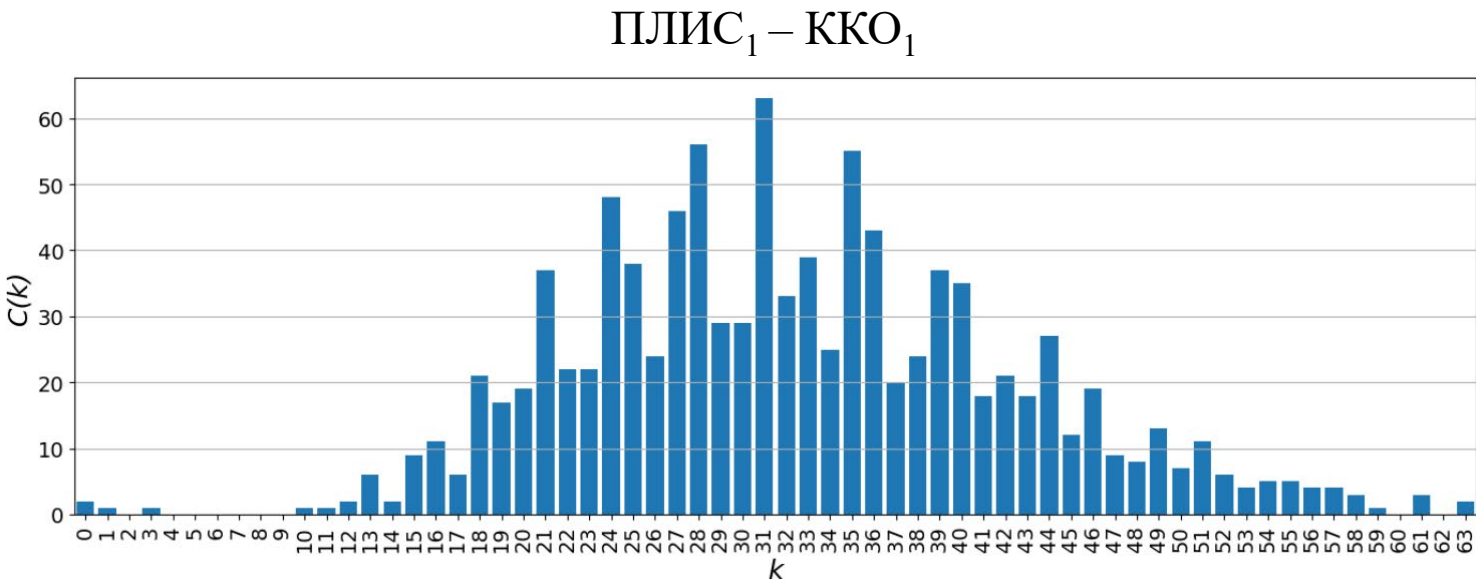
$$p(k) = \frac{C(k)}{T}$$

Далее вычисляется информационная энтропия:

$$H = - \sum_{k=0}^{2^q-1} p(k) \log_2 p(k)$$

Единообразие можно определить как:

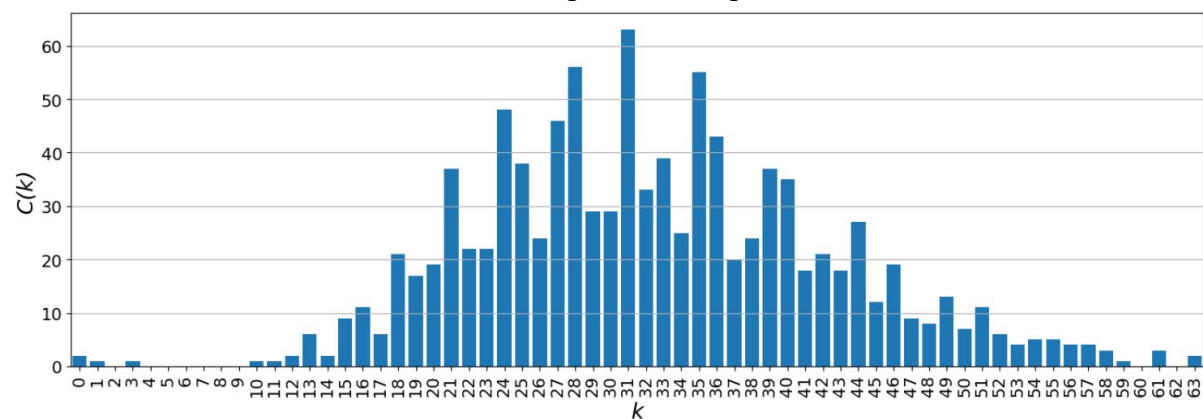
$$Uniformity = \frac{H}{q} \in [0, 1]$$



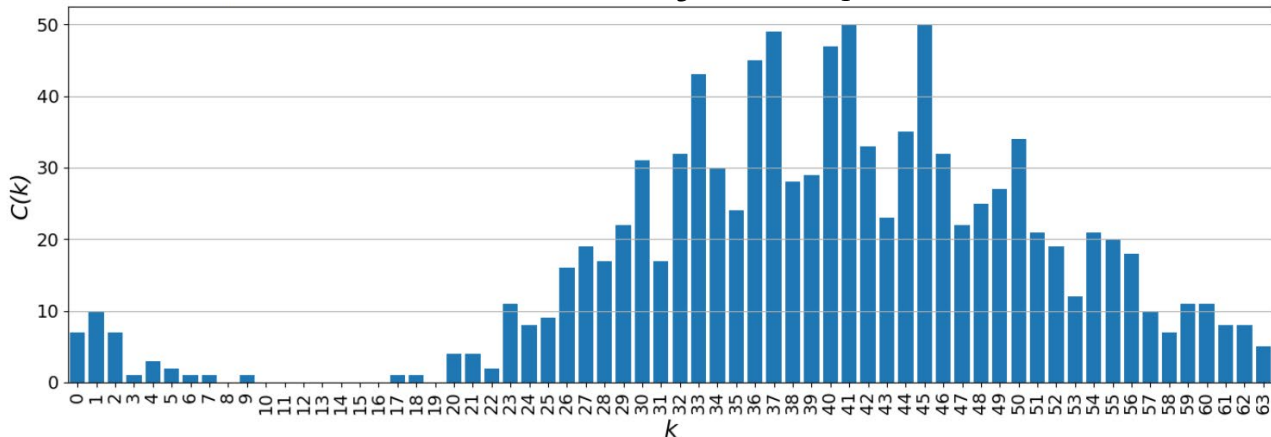
Значения характеристики единообразия

	ККО ₁	ККО ₂	ККО ₃	ККО ₄
ПЛИС ₁	0,871	0,896	0,860	0,916
ПЛИС ₂	0,883	0,906	0,874	0,922
ПЛИС ₃	0,889	0,908	0,870	0,924
ПЛИС ₄	0,886	0,902	0,867	0,919

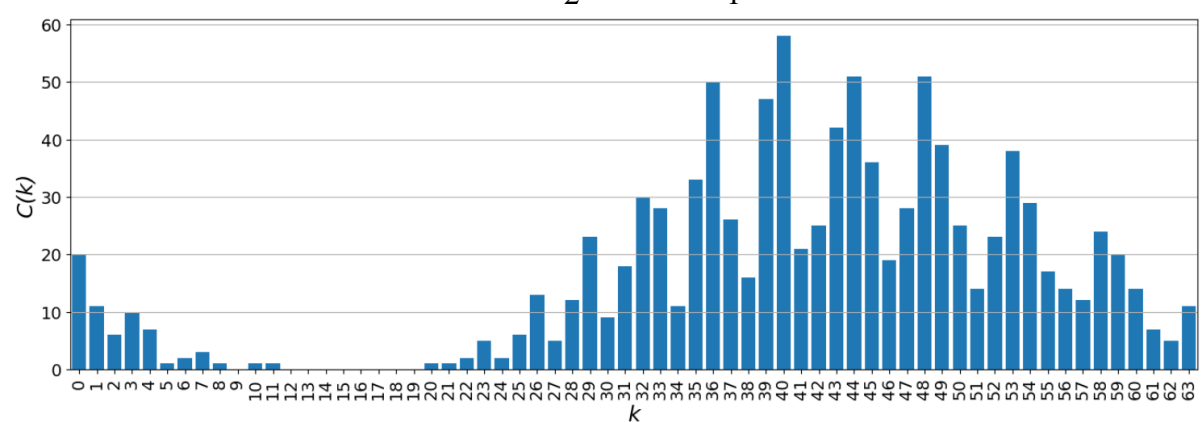
ПЛИС₁ – ККО₁



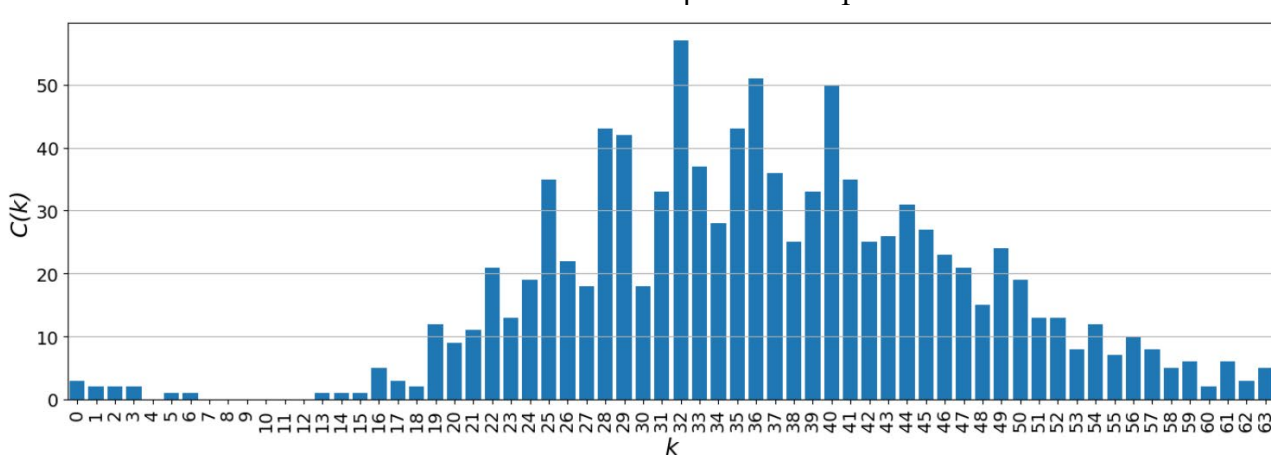
ПЛИС₃ – ККО₁



ПЛИС₂ – ККО₁

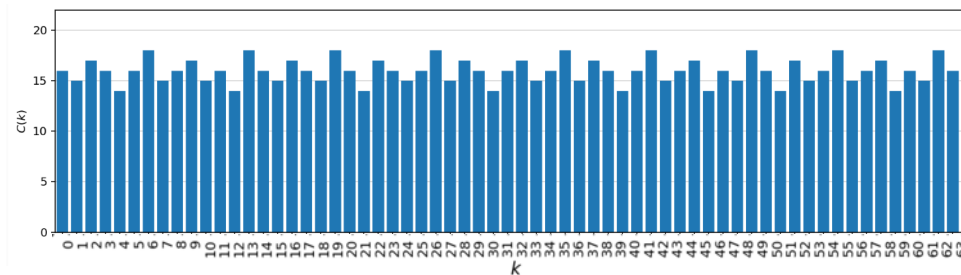
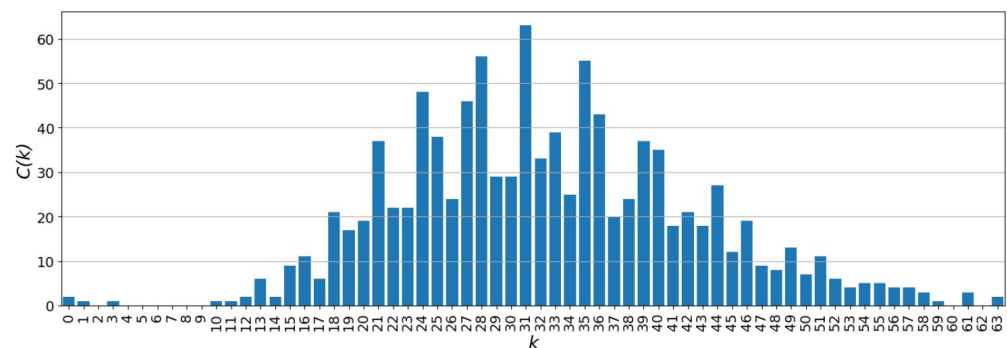


ПЛИС₄ – ККО₁



Дальнейшие задачи

1. Методами постобработки привести единообразие к равномерному.



2. Методами постобработки увеличить метрику уникальности до 0,5.

Межкристальная уникальность:

$KKO_1 - 0,482964,$
 $KKO_2 - 0,478217,$
 $KKO_3 - 0,479791,$
 $KKO_4 - 0,482322.$

Внутрикристальная уникальность:

$ПЛИС_1 - 0,427734,$
 $ПЛИС_2 - 0,420058,$
 $ПЛИС_3 - 0,419027,$
 $ПЛИС_4 - 0,427544.$

→ 0,5

3. Метрики стабильности увеличить до 1,0.



Министерство образования Республики Беларусь

EDA
Conference

Компьютерное
проектирование
в электронике

Белорусский государственный университет информатики и радиоэлектроники

СПАСИБО ЗА ВНИМАНИЕ

Докладчик:

Бурко Лиана Александровна

Руководитель:

докт. техн. наук, проф. Иванюк А.А.

Минск 2026