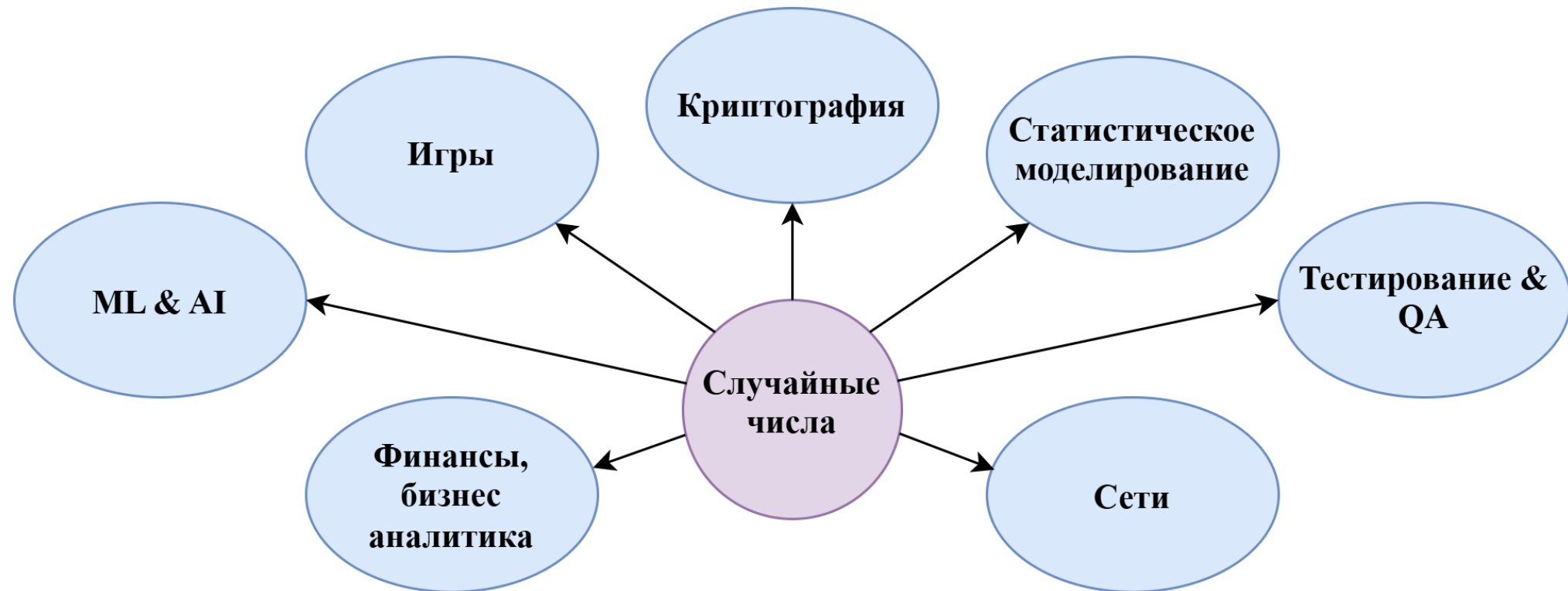


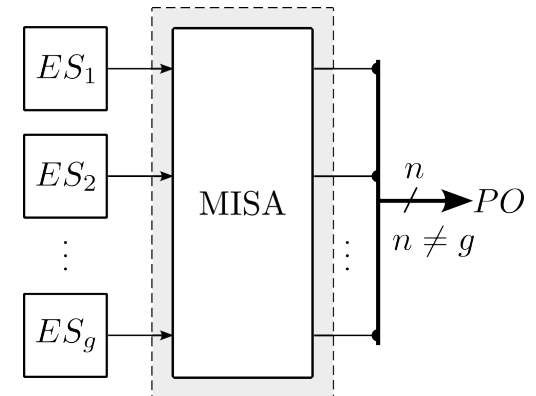
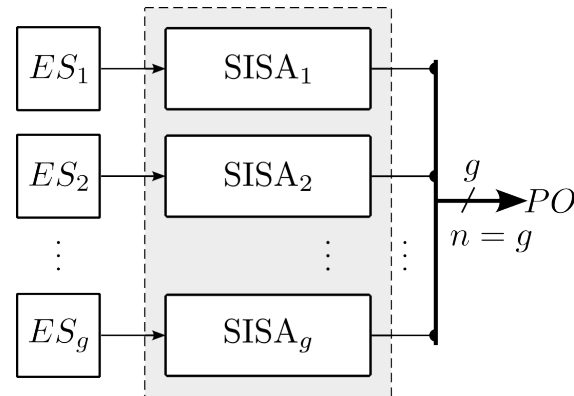
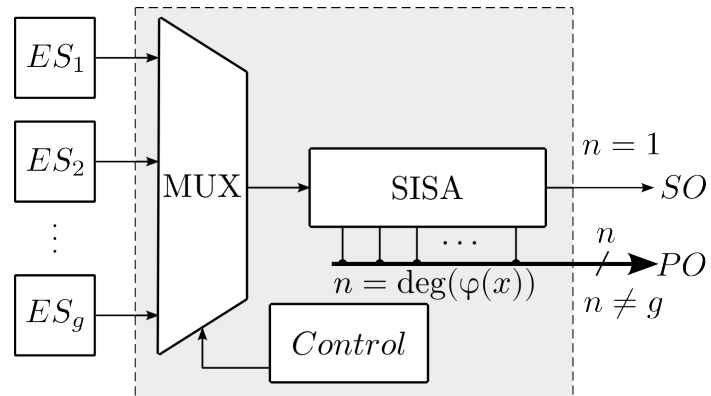
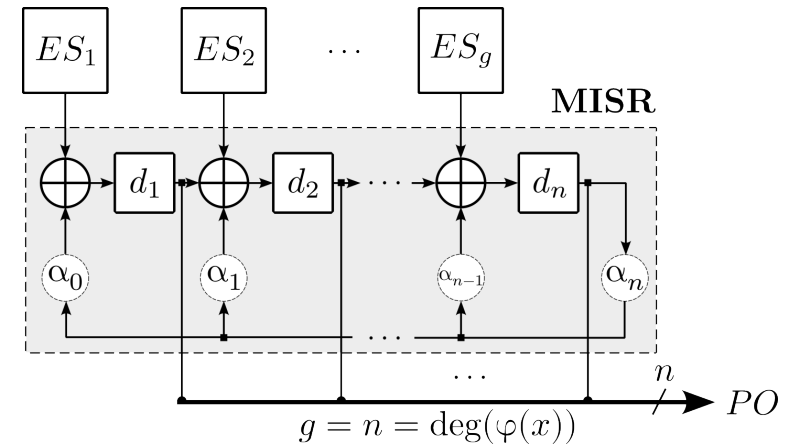
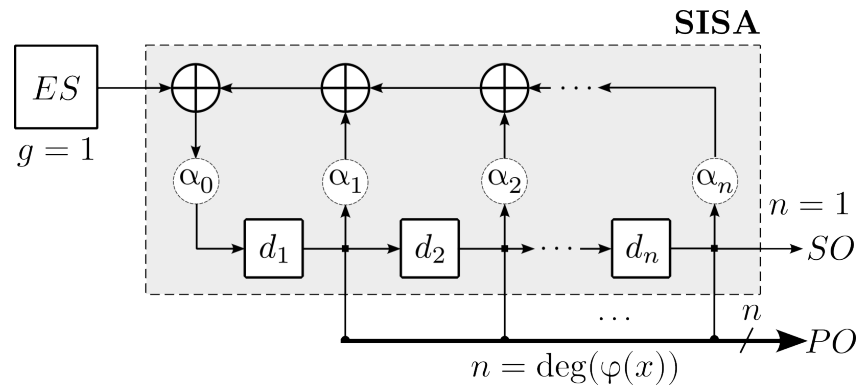
СРАВНЕНИЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ СЛУЧАЙНЫХ ЧИСЕЛ, ФОРМИРУЕМЫХ ПРИ ПОСТОБРАБОТКЕ СХЕМАМИ НА БАЗЕ МНОГОКАНАЛЬНОГО СИГНАТУРНОГО АНАЛИЗАТОРА И SHA-1

Петровский Д.А., аспирант кафедры информатики БГУИР
Иванюк А.А., д.т.н, профессор кафедры информатики БГУИР

Области применения случайных чисел

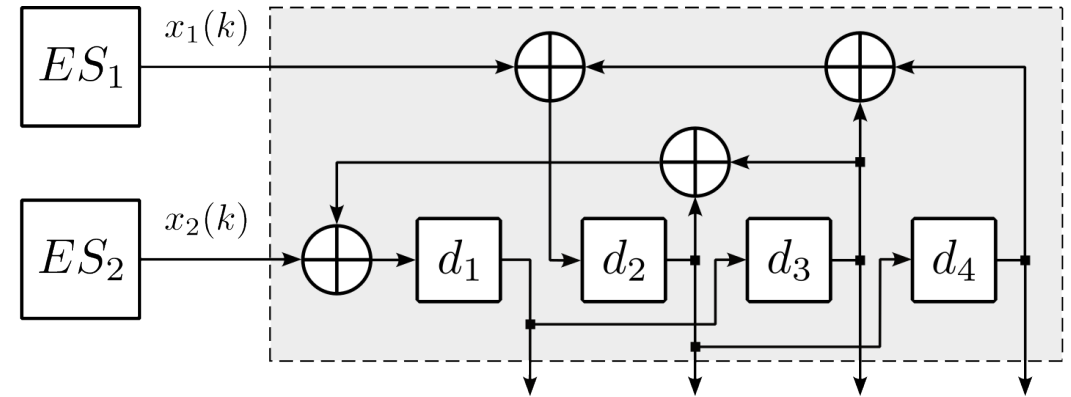


Схемы постобработки на базе LFSR



Недостатки схемы на базе MISA

- Многоканальный сигнатурный анализатор (MISA¹) — применяется в компактном тестировании для анализа реакций тестируемого устройства. Синтез схемы осуществляется на базе примитивного и неприводимого порождающего полинома.
- **Побочный эффект:** при последовательном сжатии старшие разряды выходного слова заполняются младшими разрядами предыдущего такта, что приводит к дублированию символов и снижению энтропии.



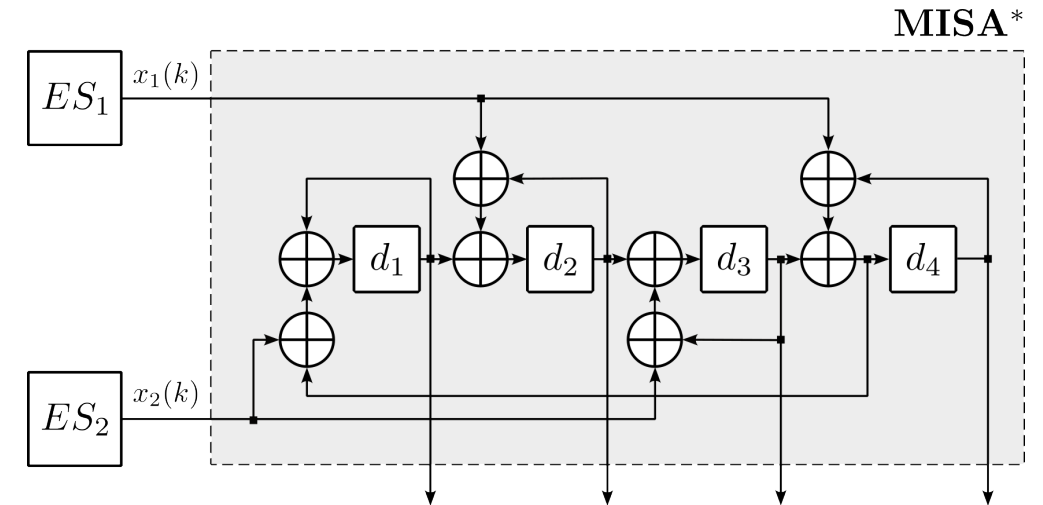
$k = 0$	$x_1(0) = a$ $x_2(0) = b$	$D(0) =$	0	0	0	0
$k = 1$	$x_1(1) = c$ $x_2(1) = d$	$D(1) =$	b	a	0	0
$k = 2$	$x_1(2) = e$ $x_2(2) = f$	$D(2) =$	$(da)_{\oplus}$	c	b	a
$k = 3$	$x_1(3) = g$ $x_2(3) = h$	$D(3) =$	$(fcb)_{\oplus}$	$(eba)_{\oplus}$	$(da)_{\oplus}$	c
$k = 4$		$D(4) =$	$(hebd)_{\oplus}$	$(gdac)_{\oplus}$	$(fcb)_{\oplus}$	$(eba)_{\oplus}$

Принцип пересинхронизации

Решение — пересинхронизация: тактовая частота MISA в j раз выше частоты обновления данных от ES. Коэффициент сжатия во времени j : за период одного входного символа схема выполняет j тактов, многократно применяя матрицу связи и обратной связи к одному значению, в следствии чего устраняются линейные корреляции. Поведение итоговой схемы в матричном виде описывается выражением:

$$\mathbf{D}(k+1) = \mathbf{C}^{j \cdot g} \cdot \mathbf{D}(k) \oplus \left[\sum_{i=1}^{g \cdot j} \left(\mathbf{C}^{i \cdot g} \cdot \mathbf{X}_{i \bmod g}(k) \right) \right],$$

$$\mathbf{C} = \begin{bmatrix} \alpha_1 & a_2 & \cdots & a_n \\ \mathbf{I}_{n-1} & \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \end{bmatrix}; \mathbf{D}(k) = \begin{bmatrix} d_1(k) \\ d_2(k) \\ \vdots \\ d_n(k) \end{bmatrix}; \mathbf{X}_i(k) = \begin{bmatrix} x_i(k) \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$



$x_1(k)$	a	a	c	c	e	e	g	g	...
$x_2(k)$	b	b	d	d	f	f	h	h	...
ES_1, ES_2	k		$k+1$		$k+2$		$k+3$		...
MISA	t	$t+1$	$t+2$	$t+3$	$t+4$	$t+5$	$t+6$	$t+7$	$t+8$
$\mathbf{D}(t)$	$d_1(t)$	0	$(ba)_{\oplus}$	$(dab)_{\oplus}$	$(dc)_{\oplus}$	$(fcda)_{\oplus}$	$(fe)_{\oplus}$	$(hebfca)_{\oplus}$	$(hga)_{\oplus}$
	$d_2(t)$	0	a	$(cba)_{\oplus}$	$(cb)_{\oplus}$	$(edc)_{\oplus}$	$(edb)_{\oplus}$	$(gfae)_{\oplus}$	$(gfdb)_{\oplus}$
	$d_3(t)$	0	b	$(ba)_{\oplus}$	$(dab)_{\oplus}$	$(dc)_{\oplus}$	$(fcda)_{\oplus}$	$(fe)_{\oplus}$	$(hebfca)_{\oplus}$
	$d_4(t)$	0	a	a	$(cba)_{\oplus}$	$(cb)_{\oplus}$	$(edc)_{\oplus}$	$(edb)_{\oplus}$	$(gfae)_{\oplus}$
		$\mathbf{D}(k)$	$\mathbf{D}(k+1)$		$\mathbf{D}(k+2)$		$\mathbf{D}(k+3)$		$\mathbf{D}(k+4)$

Описание схемы на базе SHA-1

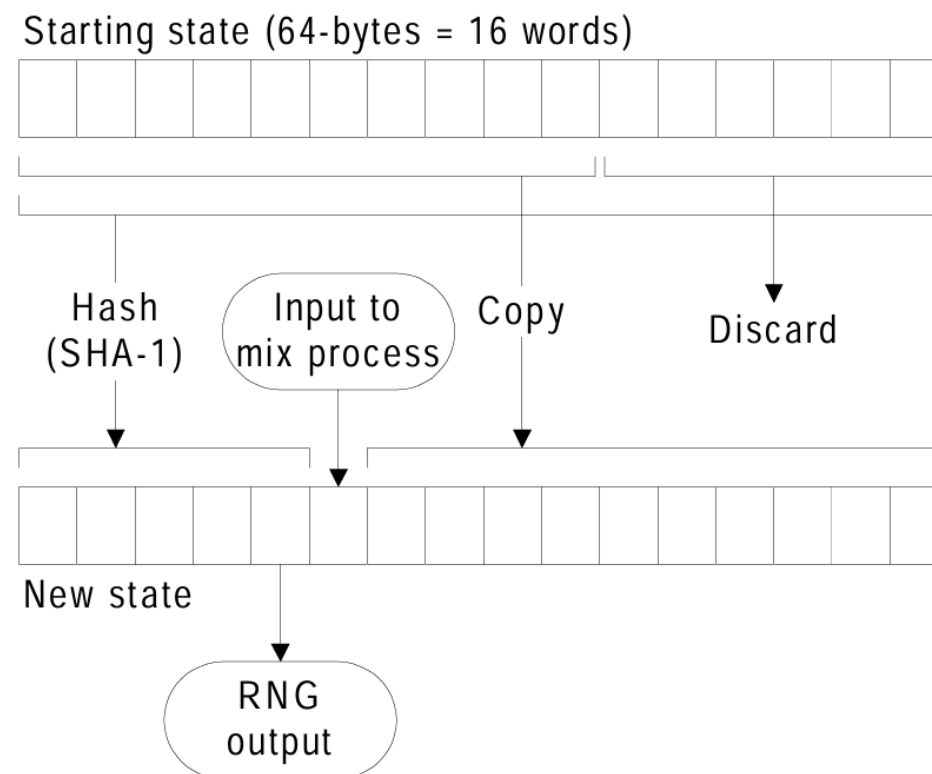
SHA-1 использовалась как функция постобработки в генераторе случайных чисел от компании Intel²:

Эффективность: объединяет входы переменного размера, генерирует независимые выходные биты с разными статистическими распределениями.

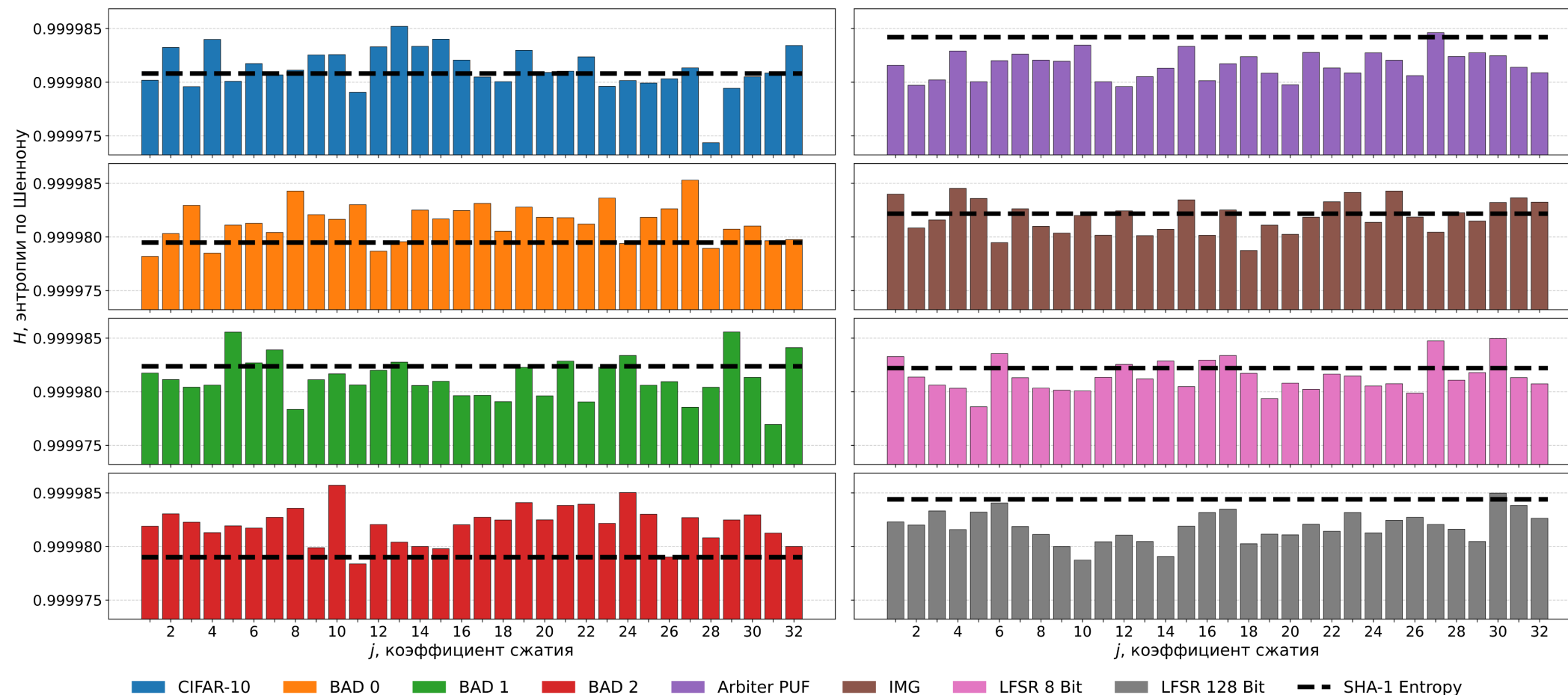
Криптостойкость: уничтожает статистическую структуру, делает вычислительно невозможным восстановление seed-состояния.

Реализация: 512-битное состояние; криптографически объединяет весь выход ГСЧ с момента инициализации.

Выход: на каждые 32 бита выхода подаётся 32 бита свежих данных от ГСЧ.



Сравнение энтропии данных обработанных схемами MISA* и SHA-1



Сравнение аппаратных затрат

В процессе исследований оценивались аппаратные затраты и максимальная расчетная частота схем постобработки на программируемых логических интегральных схемах (ПЛИС), кристалл **xc7z010-1clg400c-1**. Для схемы MISA* было разработано параметризуемое описание на HDL-языке SystemVerilog.

Тип постобработки	Аппаратные затраты		Максимальная частота
	LUT-блоков	Триггеров	МГц
MISA*	1352	512	502
SHA-1 ³	1553	1531	108

³ Verilog Implementation of the SHA-1 Cryptographic Hash Function [Electronic resource]. Mode of access: <https://github.com/secworks/sha1>.

Заключение

Проведено сравнение последовательности случайных чисел после двух схем постобработки: MISA* и эталона на SHA-1.

- При равных параметрах MISA* даёт более высокую энтропию по Шеннону чем SHA-1.
- Оценка аппаратных затрат для ПЛИС (xc7z010-1clg400c-1): MISA* требует на 15 % меньше LUT - блоков, втрое меньше триггеров и способна работать на тактовой частоте в пять раз больше по сравнению с SHA-1.
- Это делает её перспективной для энергоэффективных TRNG, включая устройства интернета вещей.

Дальнейшие исследования:

- Исследование статистических характеристик обработанных последовательностей при изменении конфигурации MISA в процессе постобработки
- Анализ методов синтеза схем на базе LFSR структур.

Благодарность: Авторы выражают искреннюю благодарность резиденту ПБТ 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.

Спасибо за внимание