CC BY

http://dx.doi.org/10.35596/1729-7648-2026-24-5-84-92

УДК 004.312

СХЕМА ПОСТОБРАБОТКИ СЛУЧАЙНЫХ ЧИСЕЛ НА БАЗЕ МНОГОВХОДОВОГО СИГНАТУРНОГО АНАЛИЗАТОРА

Д. А. ПЕТРОВСКИЙ, А. А. ИВАНЮК

Белорусский государственный университет информатики и радиоэлектроники (Минск, Республика Беларусь)

Аннотация. Проведен анализ схем постобработки на основе регистра сдвига с линейной обратной связью. Предложена модификация схемы постобработки случайных чисел с использованием многоканального сигнатурного анализатора, коэффициента сжатия во времени и изменяемого количества источников энтропии. Проанализировано влияние основных параметров схемы на энтропию обрабатываемых последовательностей и результаты статистических тестов NIST 800-22. Оценены аппаратные затраты на реализацию на программируемых логических интегральных схемах и выполнено сравнение с аналогами. Полученные результаты подтверждают перспективность схемы для применения в энергоэффективных и требовательных к аппаратным затратам генераторах истинно случайных чисел.

Ключевые слова: случайные данные, постобработка случайных чисел, многоканальный сигнатурный анализатор.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Благодарность. Авторы выражают искреннюю благодарность резиденту Парка высоких технологий 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.

Для цитирования. Петровский, Д. А. Схема постобработки случайных чисел на базе многовходового сигнатурного анализатора / Д. А. Петровский, А. А. Иванюк // Доклады БГУИР. 2026. Т. 24, № 5. С. 84–92. http://dx.doi.org/10.35596/1729-7648-2026-24-5-84-92.

RANDOM NUMBER POST-PROCESSING SCHEME BASED ON A MULTI-INPUT SIGNATURE ANALYZER

DMITRY PETROVSKY, ALEXANDER IVANIUK

Belarusian State University of Informatics and Radioelectronics (Minsk, Republic of Belarus)

Abstract. An analysis of post-processing circuits based on a linear feedback shift register is carried out. A modification of the random number post-processing circuit using a multi-input signature analyzer is proposed, which employs a time compression factor and a variable number of entropy sources. The influence of the circuit's key parameters on the entropy of processed sequences and on the results of NIST 800-22 statistical tests is analyzed. The hardware costs of implementing the circuit on programmable logic integrated circuits are estimated, and a comparison with similar circuits is performed. The results confirm the circuit's potential for use in energy-efficient and area-efficient true random number generators.

Keywords: random data, random number post-processing, multi-input signature analyzer.

Conflict of interests. The authors declare that there is no conflict of interests.

Gratitude. The authors express their sincere gratitude to the High-Tech Park resident company "Engineering Center Yadro", which is one of the YADRO development centers, for providing equipment for conducting experiments as part of the joint educational laboratory with the Belarusian State University of Informatics and Radioelectronics.

For citation. Petrovsky D., Ivaniuk A. (2026) Random Number Post-Processing Scheme Based on a Multi-Input Signature Analyzer. *Doklady BGUIR*. 24 (5), 84–92. http://dx.doi.org/10.35596/1729-7648-2026-24-5-84-92 (in Russian).

Введение

Случайные числа играют ключевую роль в криптографии, статистическом моделировании, игровой индустрии и других приложениях. Они делятся на псевдослучайные (PRN, pseudorandom number), генерируемые математическими алгоритмами, и истинно случайные (TRN, true random number), получаемые в ходе измерения характеристик неуправляемых физических процессов. Современные генераторы истинно случайных чисел (TRNG, true random number generator) могут использовать, например, радиоактивный распад, метастабильность элементов памяти, фазовое дрожание (джиттер) периодических сигналов и другие нестационарности [1]. Данные процессы позволяют получать последовательности чисел, которые нельзя рассчитать или предсказать, основываясь на элементах самой последовательности, в отличие от детерминированных PRN-последовательностей. Согласно рекомендациям National Institute of Standards and Technology (NIST), структура TRNG включает источник энтропии (ES, entropy source), блок тестирования и схему постобработки. Поскольку выходные биты ES часто имеют неравномерное распределение, для его коррекции применяют различные алгоритмы: корректор фон Неймана, XOR-преобразование, LFSR-структуры (linear-feedback shift register), а также криптографические примитивы (шифрование и хеш-функции) [2].

В статье проведен сравнительный анализ различных схем постобработки на основе LFSR-структур, выявляются их ключевые недостатки и предлагается модифицированная архитектура, которая характеризуется низкими аппаратными затратами и обеспечивает выходную последовательность с уровнем энтропии, сопоставимым с более ресурсоемкими криптографическими методами.

Схемы постобработки на базе LFSR-структур

Синтез схем на базе LFSR-структур основывается на характеристическом полиноме $\varphi(x)$, где разрядность схемы $n = \deg(\varphi(x))$. Промежуточные n разрядов случайного числа хранятся на элементах памяти $d_i \in \{0,1\}$ $(i = \overline{1,n})$ и они же являются выходным n-разрядным числом при параллельном выводе *PO*, тогда как при поточном режиме значение на выходе *SO* копируется из d_n ячейки памяти. Обязательным условием для синтеза схем постобработки является примитивность и неприводимость характеристического полинома. Основные варианты схем: одновходовой сигнатурный анализатор (SISA, single-input signature analyzer), многовходовой регистр сдвига (MISR, multiple input shift register) и многовходовой сигнатурный анализатор (MISA, multi-input signature analyzer) [3].

Схемы постобработки показаны на рис. 1. SISA (рис. 1, *a*) обрабатывает однобитный поток в двух режимах: последовательном (побитовый вывод) или параллельном (вывод n-битного слова). MISR (рис. 1, *b*) обрабатывает параллельно g входных каналов от однобитных ES, формируя n-битное слово за такт, причем $g = n$. Многоканальные конфигурации схем на базе SISA представлены на рис. 1, *c*–*d*. На рис. 1, *c* для каждого однобитного ES используется отдельный SISA, формирующий свой битовый поток; итоговая разрядность равна числу ES ($g = n$), каналы независимы. На рис. 1, *d* применяется один SISA, на вход которого через мультиплексор подаются биты от всех ES, что позволяет формировать n-разрядное слово при любом числе входных каналов g. Обобщенная схема MISA (рис. 1, *e*) обрабатывает параллельно g входных каналов и выдает n-битное слово за один такт, что значительно быстрее последовательной обработки (рис. 1, *d*). В отличие от MISR, здесь соотношение g и n может быть произвольным, что дает большую гибкость.

Качество выходной последовательности в LFSR-постобработке можно повысить за счет увеличения длины сжимаемой последовательности, числа входов g или разрядности n, но это ведет к росту времени, аппаратных затрат и числа тестовых блоков. Смягчить эти ограничения позволяют структуры MISR и MISA за счет параллельной обработки, что резко сокращает время формирования n-битного слова. Таким образом, в условиях жестких ограничений по площади

и энергопотреблению, типичных для современных TRNG, разработка компактных и эффективных схем постобработки остается актуальной. LFSR-структуры являются перспективным решением, поскольку сочетают малый размер с достаточным качеством выходной последовательности для целевых приложений.

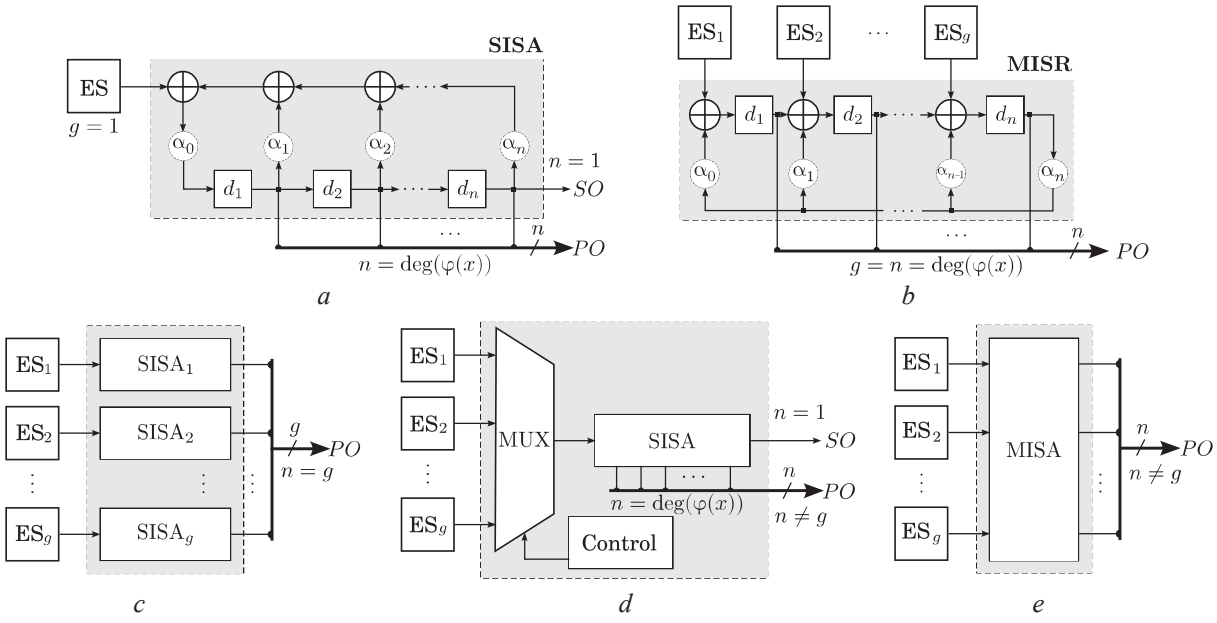


Рис. 1. Схемы постобработки на основе LFSR-структур: *a* – SISA; *b* – MISR; *c* – параллельная поточная обработка ES на основе SISA; *d* – SISA с последовательным выбором ES; *e* – MISA

Fig. 1. Post-processing schemes based on LFSR-structures: *a* – SISA; *b* – MISR; *c* – parallel stream processing of ES based on SISA; *d* – SISA with sequential ES selection; *e* – MISA

Модификация схемы MISA для постобработки случайных данных

Модификация MISA (рис. 1, *e*) на базе LFSR снижает сложность за счет уменьшения числа ES и тестовых блоков при сохранении качества, используя условие $g < n$. Однако это вызывает дублирование старших разрядов и снижение качества выходной последовательности, что требует устранения.

Методы синтеза для режима SISA с произвольным g описаны в [4], а работа схемы задается матричным выражением:

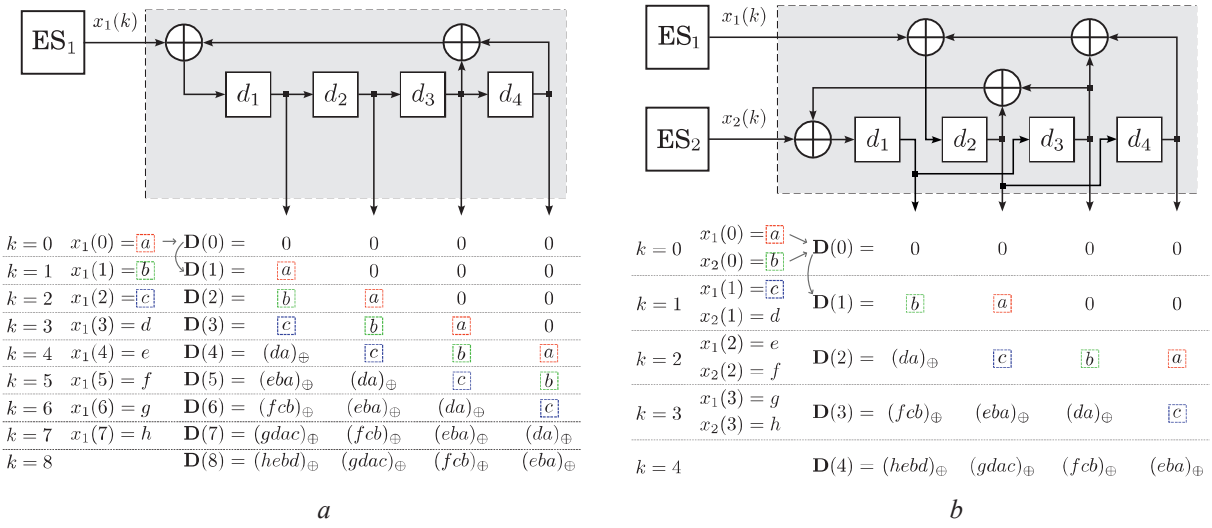
$$\mathbf{D}(k+1) = \mathbf{C}^g \cdot \mathbf{D}(k) \oplus \left[\bigoplus_{i=1}^{g} \left(\mathbf{C}^{g-i} \cdot \mathbf{X}_i(k) \right) \right];$$

$$\mathbf{C} = \begin{bmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \multicolumn{3}{c}{\mathbf{I}_{n-1}} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} \end{bmatrix}; \qquad \mathbf{D}(k) = \begin{bmatrix} d_1(k) \\ d_2(k) \\ \vdots \\ d_n(k) \end{bmatrix}; \qquad \mathbf{X}_i(k) = \begin{bmatrix} x_i(k) \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{1}$$

где $\mathbf{C}$ – матрица сдвига и обратной связи LFSR, включающая коэффициенты характеристического полинома α_i ($i = \overline{1,n}$); $\mathbf{D}(k)$ – n-разрядное двоичное слово, являющееся состоянием SISA в k-й момент времени; $x_i(k)$ – значение символа на входе SISA в k-й момент времени, которое можно представить в виде вектора $\mathbf{X}_i(k)$.

Представленное выражение для $g = 1$ описывает состояние одноканального сигнатурного анализатора при сжатии очередного символа: $\mathbf{D}(k+1) = \mathbf{C} \cdot \mathbf{D}(k) \oplus \mathbf{X}_1(k)$.

Приведем пример реализации и функционирования схемы MISA согласно (1) для $\varphi(x) = x^4 + x^3 + 1$ и количества каналов $g = 2$. Сперва рассмотрим схему SISA, которая сжимает последовательность бинарных символов от источника ES_1 (рис. 2, *a*).



a *b*

Рис. 2. Структурная схема и пример функционирования: *a* – SISA; *b* – MISA
Fig. 2. Block diagram and example of operation: *a* – SISA; *b* – MISA

Символы $x_1(k)$ ($k = \overline{0,7}$) обозначены в алфавитном порядке от *a* до *h*. Для их сжатия схеме SISA требуется восемь тактов (нулевой такт является инициализирующим). Как видно из рис. 2, на первых шести тактах на выходах наблюдаются исходные символы в явном виде, что потенциально может снизить качество выходной последовательности. На последующих тактах формируются только линейные комбинации символов, представленные в компактной нотации суммы по модулю два. Например, сумма $f \oplus c \oplus b$ в компактной нотации обозначена как $(fcb)_{\oplus}$. На рис. 2, *b* представлена схема двухканального MISA, структура которой синтезируется на основе выражений, описывающих значения разрядов d_i ($i = \overline{1,4}$) базовой схемы SISA на каждом втором (g = 2) такте работы:

$$\mathbf{D}(k+1) = \mathbf{C}^2 \cdot \mathbf{D}(k) \oplus \mathbf{C}^1 \cdot \mathbf{X}_1(k) \oplus \mathbf{C}^0 \cdot \mathbf{X}_2(k);$$

$$\mathbf{D}(k+1) = \left[x_2(k) \oplus d_2(k) \oplus d_3(k) \quad x_1(k) \oplus d_3(k) \oplus d_4(k) \quad d_1(k) \quad d_2(k) \right]^T.$$

Таким образом, схема MISA выполняет сжатие двух символов $x_1(k)$ и $x_2(k)$, поступающих от двух источников ES_1 и ES_2 за один такт, давая результат, эквивалентный последовательному сжатию двух символов $x_1(k)$ и $x_1(k+1)$ от одного источника ES_1.

Для устранения повторяющихся символов в выходной последовательности предлагается использовать пересинхронизацию схемы MISA. Идея заключается в том, чтобы тактовая частота работы MISA в j раз превышала частоту обновления данных от ES. Таким образом, за время генерации одного нового входного символа схема MISA успеет выполнить j тактов, «сжимая» это значение во времени для формирования следующего n-разрядного выходного слова $\mathbf{D}(k+1)$. Параметр j назовем коэффициентом сжатия во времени. Тогда отсчет времени t функционирования MISA будет соответствовать отсчету времени $k = \lfloor t/j \rfloor$ ($k, t \in \mathbb{Z}_{\geq 0}$, $j \in \mathbb{Z}^+$) генерирования символов от источников энтропии. На рис. 3 показан процесс формирования выходной последовательности для схемы с рис. 2, *b* для случая j = 2.

Из рис. 3 видно, что в отличие от схемы на рис. 2, *b* уже на втором такте работы схемы MISA на выходе отсутствуют исходные символы от источников энтропии. Таким образом, пересинхронизация схемы MISA может способствовать улучшению качества обрабатываемой последовательности символов.

Поскольку входные символы постоянны на протяжении сжатия, возможен переход из временно́й области в пространственную путем изменения схемы MISA так, чтобы операции с рис. 3 выполнялись за один такт. Это достигается модификацией формулы (1): увеличением числа итераций с g до $j \cdot g$ и взятием x_i с индексом канала по модулю g, что обеспечивает сжатие повторяющихся символов. В итоге работа модифицированной схемы описывается выражением

$$\mathbf{D}(k+1) = \mathbf{C}^{j \cdot g} \cdot \mathbf{D}(k) \oplus \left[\bigoplus_{i=1}^{j \cdot g} \left(\mathbf{C}^{j \cdot g - i} \cdot \mathbf{X}_{i \bmod g}(k) \right) \right]. \quad (2)$$

$x_1(k)$	a	a	c	c	e	e	g	g	$\cdots$
$x_2(k)$	b	b	d	d	f	f	h	h	$\cdots$
$\mathrm{ES}_1,\ \mathrm{ES}_2$	k		$k+1$		$k+2$		$k+3$		$\cdots$
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	b	$(ba)_\oplus$	$(dab)_\oplus$	$(dc)_\oplus$	$(fcda)_\oplus$	$(fe)_\oplus$	$(hebfca)_\oplus$	$(hga)_\oplus$
$d_2(t)$	0	a	a	$(cba)_\oplus$	$(cb)_\oplus$	$(edc)_\oplus$	$(edb)_\oplus$	$(gfae)_\oplus$	$(gfdb)_\oplus$
$d_3(t)$	0	0	b	$(ba)_\oplus$	$(dab)_\oplus$	$(dc)_\oplus$	$(fcda)_\oplus$	$(fe)_\oplus$	$(hebfca)_\oplus$
$d_4(t)$	0	0	a	a	$(cba)_\oplus$	$(cb)_\oplus$	$(edc)_\oplus$	$(edb)_\oplus$	$(gfae)_\oplus$
	$\mathbf{D}(k)$		$\mathbf{D}(k+1)$		$\mathbf{D}(k+2)$		$\mathbf{D}(k+3)$		$\mathbf{D}(k+4)$

Рис. 3. Процесс формирования выходной последовательности схемы MISA с пересинхронизацией
Fig. 3. The process of generating the output sequence of the MISA scheme with resynchronization

Для схемы MISA, показанной на рис. 2, *b*, приведем эквивалентную схему, реализующую двукратное сжатие символов ($j = 2$), поступающих от ES, как было показано на рис. 3. Пример модифицированной схемы MISA* на основе (2) приведен на рис. 4.

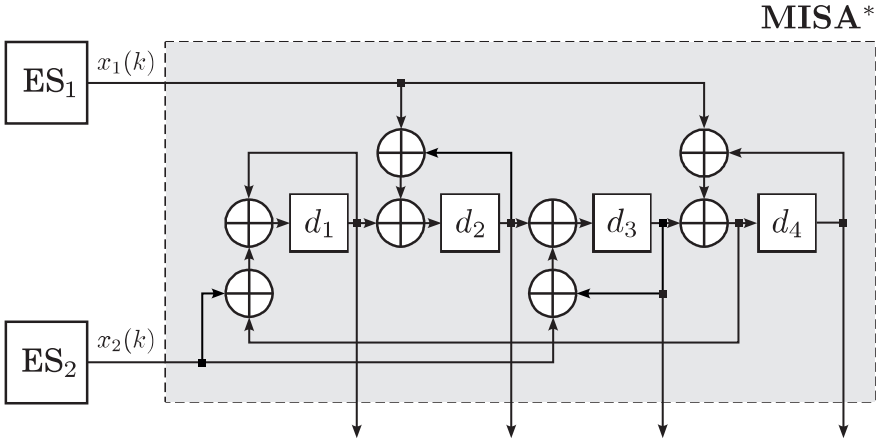


Рис. 4. Пример модифицированной схемы MISA*
Fig. 4. An example of a modified MISA* scheme

Показанная модификация схемы постобработки на базе MISA является альтернативной структурой с меньшим числом используемых однобитных ES и равной разрядностью выходного слова до модификации, т. е. $g < n$, при сохранении качества генерируемой случайной последовательности за счет устранения дублирования данных в выходном результате.

Сравнение и тестирование модифицированной схемы MISA*

Для анализа статистических свойств предложенной схемы MISA (MISA*) и классических SISA, MISA, MISR были разработаны программная модель на языке программирования C, реализующая выражение (2), и стенд для проведения экспериментов. В качестве референса использовалась схема SHA-1 из TRNG Intel [5]. Оценка проводилась по энтропии Шеннона и тестам NIST 800-22 на наборах данных по $8 \cdot 10^8$ бит (табл. 1), включающих преобразованные в поток бит изображения, псевдослучайные последовательности и последовательности, сгенерированные схемотехнической реализаций физически неклонируемой функции (ФНФ).

Изначально исследовали влияние характеристического полинома $\varphi(x)$, числа каналов g и коэффициента сжатия j на энтропию. Использовали шесть полиномов 32-й степени с шестнадцатеричными коэффициентами (poly = (0x80000057, 0x80000062, 0x9D7826E1, 0xBD9D339, 0xFB3CFCDF, 0x80003474)), где каждый бит 32-битного слова соответствовал коэффициенту α_i полинома. Эксперимент проводился на наборе CIFAR-10 при $g \in \{3,4,5\}$ и $j = \overline{1,32}$.

Таблица 1. Наборы данных, использованных в экспериментах
Table 1. Datasets used in the experiments

Набор данных	Энтропия H	Описание
CIFAR-10[1]	0,9889	60 000 цветных RGB-изображений размером 32×32 пикселя, преобразованных в последовательный поток бит
IMG[2]	0,9302	Широкоформатное RGB-изображение размером 6576×5695 пикселей, преобразованное в последовательный поток бит
LFSR-128	0,9999	М-последовательность, сгенерированная схемой LFSR с полиномом $x^{128}+x^{127}+x^{126}+x^{121}+1$, начальное значение – произвольное
Arbiter-PUF	0,9454	Данные сгенерированы на базе схемотехнической реализации ФНФ типа арбитр [6]
BAD-0	0,0452	Набор данных, полученный программным методом с искусственно низкой энтропией. Набор состоит из 10^6 нулевых подпоследовательностей, в которых псевдослучайным образом инвертировались биты
BAD-1	0,1282	
BAD-2	0,2476	

На рис. 5 показана зависимость энтропии схемы MISA* от коэффициента сжатия j, числа каналов g и полиномов $\varphi(x)$. При малых g рост j повышает энтропию за счет устранения дублей данных. При увеличении g влияние j и вида полинома становится незначительным. Так, для $g = 3$ и $j > 10$ энтропия достигает предела с матожиданием $\mu = 0{,}99981779$ и $\sigma = 0{,}00001769$. Аналогичные насыщения наблюдаются при $g = 4$ ($j > 7$) и $g = 5$ ($j > 6$) с близкими оценками μ и σ. Указанные закономерности сохраняются и для других наборов данных.

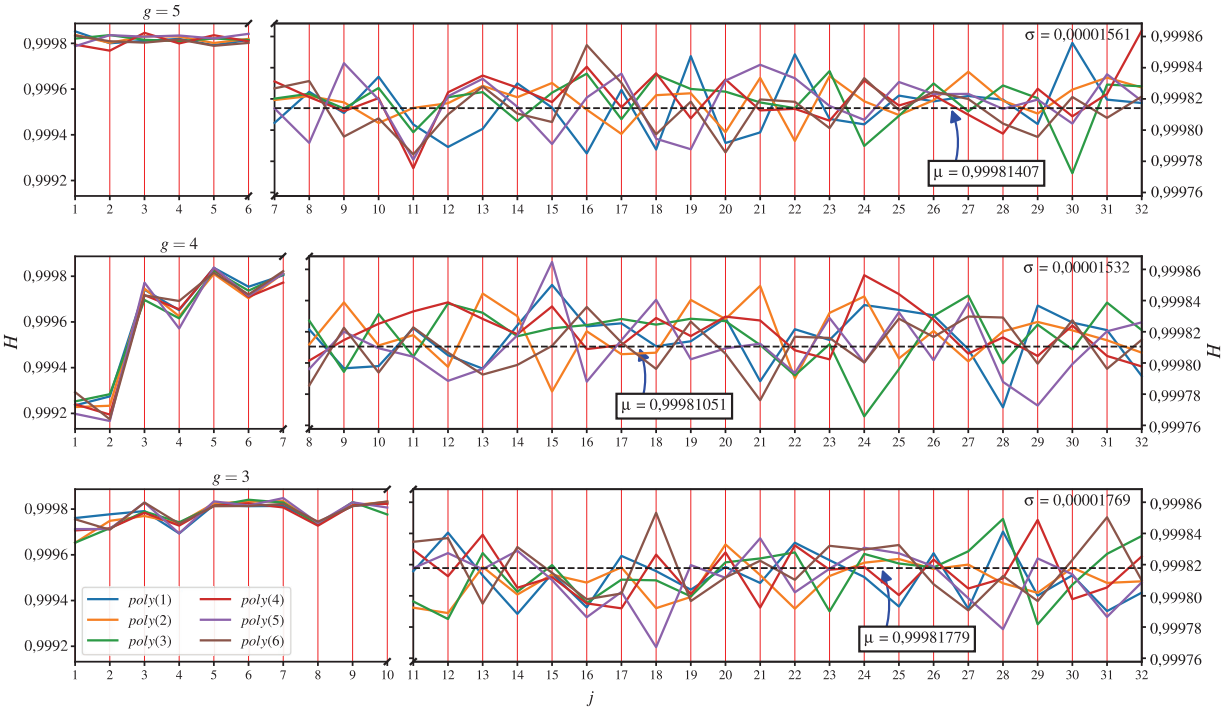


Рис. 5. Изменение энтропии от выбранного порождающего полинома, числа входных каналов и коэффициента сжатия схемы MISA*
Fig. 5. Change in entropy from the selected generator polynomial, the number of input channels and the compression ratio of the MISA* scheme

В итоге сравнивались результаты набора статистических тестов по NIST 800-22 для MISA* и аналогов: SISA (рис. 1, *c*), MISA (рис. 1, *e*), MISR (рис. 1, *b*) и SHA-1. Параметры схем, используемые в эксперименте: коэффициенты полинома $\varphi(x)$ в шестнадцатеричном виде 0x80000057; $n = 32$; количество входных каналов $g = 32$ для SISA, MISR, SHA-1, $g = 4$ для MISA*и MISA; коэффициент сжатия для MISA* $j = 17$. На программном стенде все наборы данных (табл. 1)

[1] The CIFAR-10 Dataset [Electronic resource]. Mode of access: https://www.cs.toronto.edu/~kriz/cifar.html.
[2] Босх, И. Страшный суд / И. Босх. Mode of access: https://gallerix.ru/storeroom/1400476940/N/505984321/.

обрабатывались моделями схем постобработки, после чего усекались до минимальной длины $8 \cdot 10^8$ бит. Каждый набор разбивался на 800 подпоследовательностей по 10^6 бит и тестировался по NIST 800-22. В табл. 2 приведен процент пройденных тестов для всех подпоследовательностей по наборам данных из табл. 1 и схем постобработки.

Таблица 2. Результаты тестов по NIST 800-22 для наборов из табл. 1 и схем постобработки
Table 2. NIST 800-22 test results for the sets in Tab. 1 and post-processing schemes

Схема постобработки	Тест по NIST 800-22 для набора данных, %						
	BAD-0	BAD-1	BAD-2	IMG	CIFAR-10	Arbiter-PUF	LFSR-128
Без обработки	0	0	0,04	5,68	11,78	21,97	98,46
SISA	**98,43***	**98,43***	98,43	98,47	98,41	98,43	98,42
MISR	0,69	1,29	2,36	4,48	4,90	4,80	4,50
MISA	14,37	14,32	14,18	14,69	14,59	14,86	15,24
MISA*	98,41	98,42	**98,45***	**98,83***	**98,93***	**98,97***	**99,00***
Референсная схема							
SHA-1	98,97	98,99	98,99	98,95	99,00	98,96	98,97
*Максимальный процент пройденных тестов по NIST 800-22 для набора данных среди схем на базе LFSR-структур.							

Согласно табл. 2, схемы SHA-1, SISA и предложенная MISA* показали высокий процент прохождения тестов NIST для всех исходных последовательностей. MISA* существенно превосходит MISA и MISR, обеспечивая улучшение статистических характеристик на уровне SHA-1, которая полностью соответствует NIST.

Оценка аппаратных затрат схемы MISA*

При оценке аппаратных затрат схем постобработки для кристалла программируемой логической интегральной схемы (ПЛИС) для MISA и MISA* использовалось параметризуемое HDL-описание на SystemVerilog (табл. 3). Сравнение учитывало затраты на блоки тестирования с минимальным набором Repetition Count Test и Adaptive Proportion Test [7].

Таблица 3. Оценка аппаратных затрат схем TRNG
для кристалла программируемой логической интегральной схемы xc7z010-1clg400c-1
Table 3. Hardware cost estimation of TRNG circuits
for the xc7z010-1clg400c-1 programmable logic integrated circuit crystal

Схема постобработки	Блок постобработки		Блок тестирования		Общие затраты		$F_{max}(clk)$, МГц
	LUTs	FFs	LUTs	FFs	LUTs	FFs	
SISA	64	1024	1408	864	1472	1888	446
MISR	32	32	1408	864	1440	896	**452****
MISA	**24***	32	176	108	**200***	140	390
MISA*	105	**32***	**176***	**108***	281	**140***	232
SHA-1[3]	1553	1531	1408	864	2961	2395	108
*Минимальные аппаратные затраты ресурса FPGA схемой TRNG. **Максимальная оцениваемая тактовая частота схемы TRNG.							

Анализ табл. 3 показывает, что MISA* имеет наименьшие аппаратные затраты среди всех схем – как за счет малых затрат на блоки тестирования, так и самой схемы. Ожидается, что это обеспечит и минимальное энергопотребление, что делает MISA* предпочтительной для энергоэффективных и компактных применений, например, в простых TRNG для устройств интернета вещей.

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

Заключение

1. Предложена модификация MISA с коэффициентом сжатия во времени, повышающая энтропию. Порождающий полином $\varphi(x)$ при соблюдении свойств примитивности и неприводимости слабо влияет на энтропию при разных j. Рост разрядности g увеличивает энтропию, а при малых g ее можно поднять за счет увеличения j.

2. MISA* не уступает SHA-1 и SISA по числу пройденных тестов по NIST 22-800, а аппаратные затраты для реализации на программируемой логической интегральной схеме у нее меньше, чем у SHA-1, SISA и MISR.

3. Модифицированная MISA эффективна и конкурентоспособна с SISA и SHA-1. С точки зрения соотношения аппаратных затрат и энтропии обработанных последовательностей MISA* может быть применена для энергоэффективных и компактных генераторов истинно случайных чисел.

Список литературы

1. Chai, H. A Survey of Random Number Generator: Approaches, Tests, Novel Applications in Blockchain and AI-Driven Industrial Networks / H. Chai, Q. Pan, J. Wu // *Security and Safety*. 2025. Vol. 4, Article 2025015. DOI: 10.1051/sands/2025015.
2. Fischer, V. True Random Number Generators in FPGAs / V. Fischer, F. Bernard // Computer Science, Engineering. 2011. P. 101–135. https://doi.org/10.1007/978-94-007-1338-3_5.
3. TRNG Conditioning Component with Extended Output Capability: Pat. US 0211214, IPC G06F7/58 (2006.01); CPC G06F7/588 (2013.01), G06F2207/581 (20130.1), No 18/089,370. Filing date 27.12.2022, Publ. date 27.07.2024 / A. Ivaniuk, S. Zalivaka // Applicant SK Hynix Inc. Mode of access: https://www.freepatentsonline.com/20240211214.pdf. Date of access: 20.06.2025.
4. Ярмолик, В. Н. Построение многоканальных сигнатурных анализаторов / В. Н. Ярмолик // Автоматика и телемеханика. 1985. № 1. С. 127–132.
5. Jun, B. The Intel Random Number Generator / B. Jun, P. Kocher // Cryptograph Research Inc., White Paper. 1999. Vol. 27. P. 1–8.
6. Шамына, А. Ю. Исследование временных параметров физически неклонируемой функции типа арбитр с использованием кольцевого осциллятора / А. Ю. Шамына, А. А. Иванюк // Цифровая трансформация. 2022. Т. 28, № 1. С. 27–38. DOI: 10.35596/2522-9613-2022-28-1-27-38.
7. Burko, L. Health Tests Hardware Implementation for Entropy Sources / L. Burko, M. Kaiky, A. Ivaniuk // Информационные технологии и системы 2023: материалы Междунар. науч. конф., Минск, 22 нояб. 2023 г. Минск: Белор. гос. ун-т информ. и радиоэлек., 2023. С. 119–120.

Поступила 25.08.2026 Принята в печать 14.09.2026

References

1. Chai H., Pan Q., Wu J. (2025) A Survey of Random Number Generator: Approaches, Tests, Novel Applications in Blockchain and AI-Driven Industrial Networks. *Security and Safety*. 4 (2025015). DOI: 10.1051/sands/2025015.
2. Fischer V., Bernard F. (2011) True Random Number Generators in FPGAs. *Computer Science, Engineering*. 101–135. https://doi.org/10.1007/978-94-007-1338-3_5.
3. Ivaniuk A., Zalivaka S. (2024) TRNG Conditioning Component with Extended Output Capability. *Patent US 0211214, IPC G06F7/58 (2006.01); CPC G06F7/588 (2013.01), G06F2207/581 (20130.1), No 18/089,370. Filing date 27.12.2022, Publ. date 27.07.2024. Applicant SK Hynix Inc*. Available: https://www.freepatentsonline.com/20240211214.pdf (Accessed 20 June 2025).
4. Yarmolik V. N. (1985) Design of Multichannel Signature Analyzers. *Automation and Remote Control*. (1), 127–132 (in Russian).
5. Jun B., Kocher P. (1999) The Intel Random Number Generator. *Cryptograph Research Inc., White Paper*. 27, 1–8.
6. Shamyna A. Yu., Ivaniuk A. A. (2022) Investigation of the Timing Parameters of the Arbiter-Based Physically Unclonable Function Using a Ring Oscillator. *Digital Transformation*. 28 (1), 27–38. https://doi.org/10.35596/2522-9613-2022-28-1-27-38 (in Russian).
7. Burko L., Kaiky M., Ivaniuk A. (2023) Health Tests Hardware Implementation for Entropy Sources. *Information Technologies and Systems 2023, Proceedings of the International Scientific Conference, Minsk, Nov. 22*. Minsk, Belarusian State University of Informatics and Radioelectronics. 119–120.

Received: 25 August 2026 Accepted: 14 September 2026

Вклад авторов

Петровский Д. А. спроектировал схему постобработки, реализовал программную модель схемы, выполнил аппаратную реализацию схемы для FPGA, провел экспериментальные исследования.

Иванюк А. А. определил задачи, необходимые для проведения исследований, принял участие в интерпретации результатов эксперимента.

Authors' contribution

Petrovsky D. designed the postprocessing scheme, implemented the software model of the scheme, performed hardware implementation of the scheme for FPGA, conducted experimental studies.

Ivaniuk A. defined the tasks necessary for conducting the research and took part in the interpretation of the experimental results.

Сведения об авторах

Петровский Д. А., магистр техн. наук, асп., Белорусский государственный университет информатики и радиоэлектроники

Иванюк А. А., д-р техн. наук, проф., проф. каф. информатики, Белорусский государственный университет информатики и радиоэлектроники

Адрес для корреспонденции

220013, Республика Беларусь,
Минск, ул. П. Бровки, 6
Белорусский государственный университет
информатики и радиоэлектроники
Тел.: +375 29 698-14-90
E-mail: petrovsky.dmitr@gmail.com
Петровский Дмитрий Алексеевич

Information about the authors

Petrovsky D., M. Sci. (Tech.), Postgraduate, Belarusian State University of Informatics and Radioelectronics

Ivaniuk A., Dr. Sci. (Tech)., Professor, Professor at the Department of Computer Science, Belarusian State University of Informatics and Radioelectronics

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovki St., 6
Belarusian State University
of Informatics and Radioelectronics
Tel.: +375 29 698-14-90
E-mail: petrovsky.dmitr@gmail.com
Petrovsky Dmitry