 © Авторы статьи / Authors of the article

ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ/INFORMATICS AND INFORMATION PROCESSES

DOI: https://doi.org/10.60797/IRJ.2026.173.72 EDN: MBSQDO

ПОВЕДЕНЧЕСКАЯ МОДЕЛЬ ГЕНЕРАТОРА ИСТИННО СЛУЧАЙНЫХ ЧИСЕЛ НА ОСНОВЕ JK-ТРИГГЕРА В НЕШТАТНОМ РЕЖИМЕ

Научная статья

Сабиров Н.А.[1], Юсупов Б.З.[2,] *

[1, 2] Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

* Корреспондирующий автор (bulatusupov9[at]gmail.com)

Предложена: 09.07.2026; Принята: 22.10.2026; Опубликована: 17.11.2026

Аннотация

В работе исследована возможность использования стандартного JK-триггера в метастабильном режиме в качестве генератора истинно случайных чисел для аппаратной криптографии. При одновременной подаче логических единиц на оба информационных входа в Master-ступени двухступенчатого триггера возникает состязание сигналов установки и сброса, исход которого при технологической симметрии сигнальных путей определяется тепловым шумом. Для описания этого явления предложена концептуальная модель «Весы», представляющая исход каждого такта как функцию систематической асимметрии задержек и аддитивного гауссова шума. Методом поведенческого моделирования на выборке 10^6 бит показано, что при скомпенсированной асимметрии генерируемая последовательность обладает высоким качеством случайности: смещение составило 0.0004, энтропия Шеннона — 1.0000, минимальная энтропия — 0.9989. Тесты NIST SP 800-22 (Frequency, Block Frequency, Runs) пройдены со значениями P-value от 0.17 до 0.74, автокорреляционный анализ не выявил статистически значимых зависимостей между битами. Практическая значимость предложенного подхода состоит в том, что генератор реализуется на стандартной библиотечной ячейке без схемных модификаций и цепей постобработки, что упрощает его интеграцию в ПЛИС и системы на кристалле.

Ключевые слова: генератор истинно случайных чисел, JK-триггер, состязание сигналов, тепловой шум, источник энтропии, аппаратная криптография, тесты NIST SP 800-22, поведенческое моделирование, ПЛИС.

A BEHAVIOURAL MODEL OF A TRULY RANDOM NUMBER GENERATOR BASED ON A JK TRIGGER IN AN ABNORMAL MODE

Research article

Sabirov N.A.[1], Yusupov B.Z.[2,] *

[1, 2] Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

* Corresponding author (bulatusupov9[at]gmail.com)

Suggested: 09.07.2026; Accepted: 22.10.2026; Published: 17.11.2026

Abstract

The work examines the possibility of using a standard JK trigger in a metastable mode as a true random number generator for hardware cryptography. When logic ‘1’s’ are applied simultaneously to both data inputs of the master stage of a two-stage trigger, a competition occurs between the set and reset signals; the outcome of this competition, given the technological symmetry of the signal paths, is determined by thermal noise. To describe this phenomenon, a conceptual model called ‘Scales’ has been proposed, which represents the outcome of each clock cycle as a function of systematic delay asymmetry and additive Gaussian noise. Using behavioural modelling on a sample of 10^6 bits, it has been shown that, when the asymmetry is compensated for, the generated sequence exhibits a high degree of randomness: the bias was 0.0004, the Shannon entropy was 1.0000, and the minimum entropy was 0.9989. The NIST SP 800-22 tests (Frequency, Block Frequency, Runs) were passed with P-values ranging from 0.17 to 0.74; autocorrelation analysis found no statistically significant correlations between bits. The practical significance of the suggested approach lies in the fact that the generator is implemented on a standard library cell without any circuit modifications or post-processing circuits, which simplifies its integration into FPGAs and on-chip systems.

Keywords: true random number generator, JK trigger, race condition, thermal noise, entropy source, hardware cryptography, NIST SP 800-22 tests, behavioural modelling, FPGA.

Введение

Генераторы истинно случайных чисел (ГИСЧ) — ключевой элемент аппаратной криптографии. В отличие от псевдослучайных генераторов, ГИСЧ извлекают энтропию из физических процессов и принципиально непредсказуемы [1].

Современные аппаратные средства защиты информации развиваются параллельно с методами эффективной обработки и кодирования данных. Криптографические механизмы тесно связаны не только с генерацией случайных последовательностей, но и с алгоритмами представления информации, поскольку процессы кодирования оказывают влияние на эффективность хранения, передачи и последующей обработки данных. В последние годы особое внимание уделяется разработке программно-аппаратных и учебно-лабораторных комплексов, позволяющих исследовать

 © Авторы статьи / Authors of the article

практическое применение алгоритмов кодирования информации и оценивать их эффективность при решении прикладных задач защиты информации [2].

Традиционные ГИСЧ делятся на три класса: аналоговые (шумящий диод, резистор) — громоздкие и чувствительные к наводкам; генераторы на кольцевых осцилляторах [3], [4] — требуют постобработки; metastability-based (SRAM [5], арбитры [6], [7]) — опираются на специализированные схемные блоки [8]. Общий недостаток — необходимость в нестандартных ячейках, что усложняет интеграцию в системы на кристалле (СнК) и программируемые логические интегральные схемы (ПЛИС).

В данной работе предлагается использовать стандартный JK-триггер в нештатном режиме (J=1, K=1) как источник энтропии. При одновременной подаче единиц на оба входа в Master-ступени возникает состязание сигналов Set и Reset. Если технологический разброс задержек пренебрежимо мал, исход каждого такта определяется тепловым шумом — триггер становится ГИСЧ.

Модель состязания сигналов в JK-триггере

В двухступенчатом JK-триггере (Master-Slave) [9], [10], [11] при J=1, K=1 обе перекрёстные обратные связи Master-ступени активны одновременно. Возникающее в Master-ступени состязание сигналов установки (Set) и сброса (Reset) фиксируется на входах Slave-ступени, выполняющей роль арбитра. Исход состязания определяется тем, какой из двух фронтов достигнет порога переключения первым, то есть разностью задержек распространения τ_J и τ_K соответствующих сигнальных путей.

Для анализа этого явления предложена концептуальная модель «Весы», представленная на Рис. 1. Два сигнальных пути — Set и Reset — моделируются линиями задержки с номинальными значениями τ_J и τ_K, которые сходятся к арбитру (Slave-ступени).

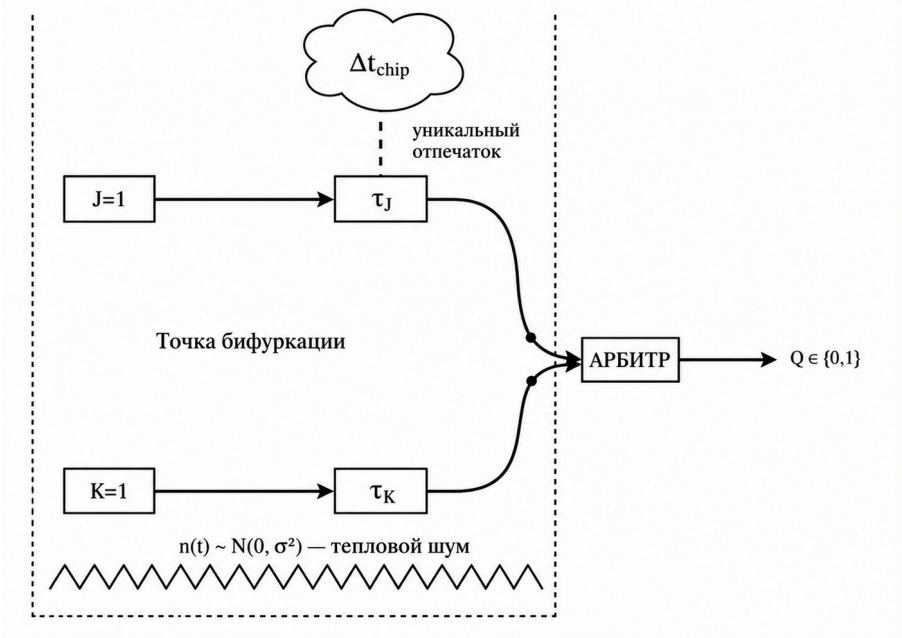


Рисунок 1 - Концептуальная модель «Весы»

DOI: https://doi.org/10.60797/IRJ.2026.173.72.1

На исход состязания влияют два фактора. Первый — систематическая асимметрия задержек Δt_{chip}, обусловленная технологическим разбросом параметров транзисторов (длина канала, толщина оксида, концентрация примесей). Эта асимметрия постоянна для данного экземпляра микросхемы и лежит в диапазоне [-1;+1] пс для типового КМОП-техпроцесса. Второй фактор — тепловой шум $\eta(t)$, моделируемый как аддитивная гауссова случайная величина с нулевым математическим ожиданием (1):

$$\eta(t) \sim N\left(0, \sigma^2\right), \tag{1}$$

где $\sigma = 0.3$ пс — среднеквадратичное отклонение, определяемое физическими параметрами схемы.

Функция исхода Ψ определяется как сумма всех факторов, влияющих на разность задержек (2):

$$\Psi = \left(\tau_J - \tau_K\right) + \Delta t_{chip} + \eta(t). \tag{2}$$

При топологической симметрии путей ($\tau_J = \tau_K$), заложенной на этапе проектирования, первое слагаемое обнуляется, и выражение упрощается до $\Psi = \Delta t_{chip} + \eta(t)$.

Точка $\Psi = 0$ является порогом принятия решения. Правило арбитража формулируется следующим образом:

$$Q = \begin{cases} 1(\text{ Set }), & \text{если } \Psi < 0 \\ 0(\text{ Reset }), & \text{если } \Psi \geq 0 \end{cases} \tag{3}$$

 © Авторы статьи / Authors of the article

Физический смысл правила (3): при $\Psi < 0$ суммарная задержка пути Set меньше, чем пути Reset — фронт установки приходит к арбитру первым и фиксирует $Q = 1$.

В зависимости от соотношения $|\Delta t_{\text{chip}}|$ и σ реализуются три качественно различных режима, проиллюстрированных на Рис. 2. Если $|\Delta t_{\text{chip}}| \square \sigma$, распределение Ψ целиком лежит по одну сторону от порога $\Psi = 0$. Исход состязания предопределён систематической асимметрией, и триггер стабильно выдаёт 0 или 1 — режим физически неклонируемой функции (PUF). Если $|\Delta t_{\text{chip}}| \approx 0$, распределение Ψ симметрично относительно порога. Исход каждого такта определяется исключительно мгновенным значением шума $\eta(t)$; вероятность P(Q=1) близка к 0.5, а последовательные биты статистически независимы. Именно этот, метастабильный, режим представляет интерес как источник энтропии для ГИСЧ. В массовой партии микросхем доля технологически симметричных экземпляров составляет доли процента, что достаточно для реализации одного генератора на кристалл.

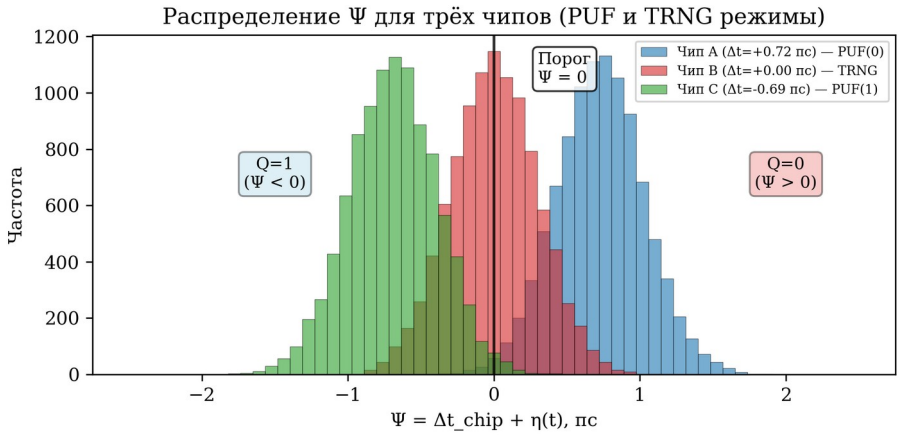


Рисунок 2 - Распределение функции исхода Ψ для трёх экземпляров JK-триггера
DOI: https://doi.org/10.60797/IRJ.2026.173.72.2

Методика оценки качества случайности

Качество ГИСЧ оценивается по трём группам критериев: энтропийным метрикам, статистическим тестам и автокорреляционному анализу.

Энтропийные метрики. Пусть p_0 и p_1 — вероятности появления нуля и единицы в выходной последовательности. Смещение (bias) определяется как $|p_1 - 0.5|$; идеальное значение 0. Энтропия Шеннона $H = -p_0 \log_2 p_0 - p_1 \log_2 p_1$ характеризует среднее количество информации на бит; максимум H=1 достигается при $p_0 = p_1 = 0.5$. Минимальная энтропия $H_{\min} = -\log_2 (\max (p_0, p_1))$ даёт консервативную оценку для криптографических приложений.

Статистические тесты. Применены три теста из батареи NIST SP 800-22 [12], рекомендованной для сертификации ГИСЧ [13]. Частотный тест (Frequency Monobit) проверяет близость доли единиц к 0.5. Частотный тест внутри блока (Frequency within Block, M=128) оценивает равномерность распределения на коротких отрезках. Тест серий (Runs) анализирует частоту чередования нулей и единиц. Тест считается пройденным, если P-value > 0.01.

Современные методы анализа цифровых потоков всё чаще основаны на технологиях обработки больших объёмов данных и интеллектуальных алгоритмах выявления отклонений. Использование моделей глубокого обучения позволяет обнаруживать скрытые закономерности и аномалии в последовательностях, формируемых в режиме реального времени, что повышает достоверность оценки качества цифровых потоков. Подобный подход демонстрирует перспективность совместного применения классических статистических критериев и современных методов интеллектуального анализа данных при оценке характеристик генераторов случайных чисел [14].

Для проверки независимости последовательных битов вычисляется автокорреляционная функция на лагах $k = 1 \ldots 100$. При уровне значимости 0.05 доверительный интервал составляет $\pm 1.96/\sqrt{N}$, где N — объём выборки. Выход за границы интервала указывает на статистически значимую зависимость.

Эксперимент

Эксперимент проведён методом поведенческого моделирования на языке Python. Параметры эксперимента приведены в Таблице 1.

Таблица 1 - Параметры эксперимента

DOI: https://doi.org/10.60797/IRJ.2026.173.72.3

Параметр	Значение
Число моделируемых экземпляров (чипов)	10

 © Авторы статьи / Authors of the article

Параметр	Значение
Объём выборки для ГИСЧ	10^6 бит
Среднеквадратичное отклонение шума	0.3 пс
Диапазон систематической асимметрии	[-1.0,+1.0] пс
Начальное значение генератора (seed)	42

При разработке и верификации аппаратных средств информационной безопасности особое значение имеют специализированные испытательные стенды, позволяющие контролировать характеристики электронных устройств и воспроизводить различные режимы их функционирования. Практика создания подобных аппаратно-программных комплексов показывает, что предварительное моделирование и последующая экспериментальная проверка существенно повышают достоверность получаемых результатов и позволяют выявлять особенности работы цифровых схем ещё до изготовления физического прототипа. Аналогичный подход используется и при разработке стендов для контроля и анализа пороговых извещателей, где значительное внимание уделяется воспроизводимости измерений, обработке экспериментальных данных и оценке корректности функционирования электронных узлов [15].

На первом этапе сформирована популяция из десяти виртуальных экземпляров JK-триггера. Для каждого экземпляра значение Δt_{chip} извлечено из равномерного распределения $U(-1.0, +1.0)$ пс и зафиксировано. Пробная выборка объёмом 10^4 бит на каждом чипе позволила идентифицировать экземпляры, предрасположенные к метастабильности. Экземпляр с $\left|\Delta t_{\text{chip}}\right| < 0.1$ пс отобран как кандидат в ГИСЧ. Отметим, что критерий $\left|\Delta t_{\text{chip}}\right| < 0.1$ пс является лишь предварительным: при граничном значении $\left|\Delta t_{\text{chip}}\right| = 0.1$ пс и $\sigma = 0.3$ пс вероятность единицы достигает $\Phi(0.1/0.3) \approx 0.63$, что не удовлетворяет требованиям к ГИСЧ. Поэтому отбор служит для сужения диапазона последующей компенсации остаточной асимметрии, а не для её устранения.

На втором этапе остаточная асимметрия отобранного экземпляра считается скомпенсированной – задано $\Delta t_{\text{chip}} = 0$. Такое значение моделирует чип после точной подстройки задержек (например, программируемыми элементами задержки) либо технологически симметричный экземпляр, у которого разброс параметров транзисторов Set- и Reset-путей пренебрежимо мал; полученные ниже характеристики следует рассматривать как предельно достижимые для метастабильного режима. Сгенерирована последовательность из 10^6 бит. Для каждого бита вычислялось значение $\Psi = \Delta t_{chp} + \eta(t)$, где $\eta(t)$ — случайная величина, распределённая по нормальному закону $N\left(0, 0.3^2\right)$. Бит фиксировался как 1 при $\Psi < 0$ и как 0 в противном случае, согласно правилу (3). Начальное значение генератора псевдослучайных чисел зафиксировано (seed=42) для обеспечения воспроизводимости.

Результаты

Энтропийные метрики. Характеристики сгенерированной последовательности приведены в Таблице 2.

Таблица 2 - Метрики качества случайности

DOI: https://doi.org/10.60797/IRJ.2026.173.72.4

Метрика	Значение
Число бит	1 000 000
Число единиц	500 394
Число нулей	499 606
P(1)	0.5004
Смещение (bias)	0.0004
Энтропия Шеннона	1.0000
Минимальная энтропия	0.9989

Смещение составило 0.0004, что в 2.5 раза ниже типового порога 0.001, применяемого к ГИСЧ без постобработки. Энтропия Шеннона достигла максимального значения 1.0000. Минимальная энтропия $H_{mm} = 0.9989$ означает, что на каждый выходной бит приходится не менее 0.9989 бита истинной случайности.

Статистические тесты NIST. Результаты тестов представлены в Таблице 3.

Таблица 3 - Результаты статистических тестов NIST SP 800-22

DOI: https://doi.org/10.60797/IRJ.2026.173.72.5

Тест	P-value	Результат
Frequency (Monobit)	0.4307	Пройден
Frequency (Block, M=128)	0.1738	Пройден
Runs	0.7442	Пройден

 © Авторы статьи / Authors of the article

Все три теста пройдены (P-value > 0.01). Значения P-value лежат в диапазоне [0.17, 0.74], вдали как от критической границы 0.01, так и от единицы, что свидетельствует об отсутствии как грубого смещения, так и искусственной «подгонки» под тесты.

Автокорреляционный анализ. Автокорреляционная функция для лагов $k = 1 \ldots 100$ представлена на Рис. 3.

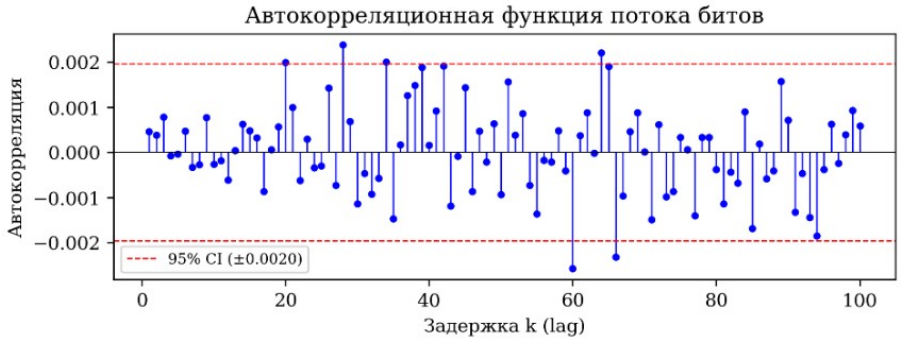


Рисунок 3 - Автокорреляционная функция потока битов с 95% доверительным интервалом
DOI: https://doi.org/10.60797/IRJ.2026.173.72.6

Анализ электрических характеристик цифровых устройств требует комплексной оценки не только статистических показателей выходной последовательности, но и стабильности поведения электронных элементов при различных режимах функционирования. Подобный подход широко применяется при экспериментальном исследовании электронных компонентов систем безопасности, где достоверность результатов определяется корректностью измерений, воспроизводимостью экспериментов и сопоставлением полученных характеристик с расчётными моделями. Использование аналогичной методологии при оценке работы генератора случайных чисел позволяет повысить объективность анализа и обеспечивает более надёжную интерпретацию экспериментальных данных [16].

Ни одно значение автокорреляции не выходит за пределы 95% доверительного интервала (±0.002), что подтверждает статистическую независимость последовательных битов.

Гистограмма распределения. Соотношение нулей и единиц в выходной последовательности показано на Рис. 4.

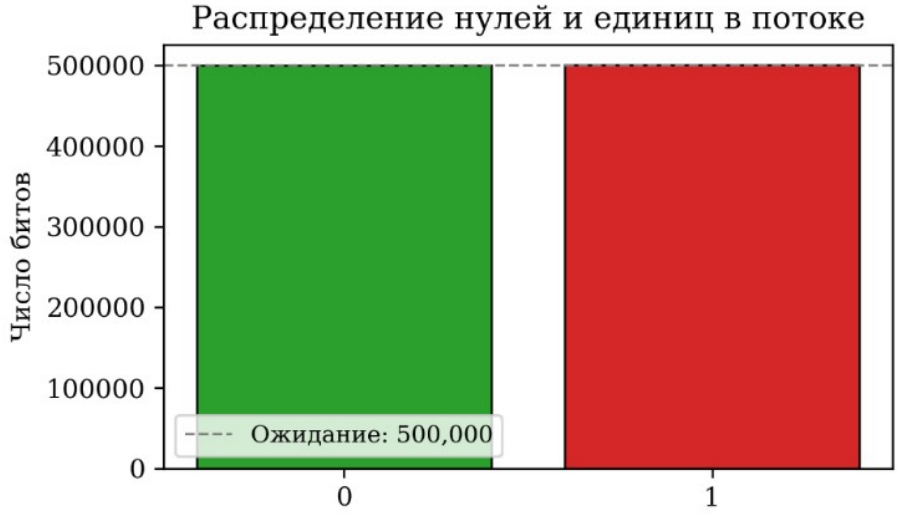


Рисунок 4 - Распределение нулей и единиц в сгенерированной последовательности
DOI: https://doi.org/10.60797/IRJ.2026.173.72.7

Разница между числом нулей (499 606) и единиц (500 394) составляет менее 0.08% от объёма выборки, что подтверждает равномерность распределения.

Полученные результаты сопоставимы с характеристиками известных ГИСЧ на метастабильных элементах. Так, в SRAM-based TRNG [5] минимальная энтропия типично составляет 0.85–0.95 бит/бит; достигнутое значение 0.9989 превышает этот диапазон. Генераторы на кольцевых осцилляторах [3], [4] обеспечивают сопоставимое качество, но требуют схем постобработки (корректор смещения, экстрактор энтропии), в то время как предложенное решение обходится без них благодаря технологической симметрии триггера.

Следует отметить следующие ограничения. Итоговые показатели качества случайности (Таблицы 2, 3) получены для случая полностью скомпенсированной систематической асимметрии и характеризуют предельно достижимый

 © Авторы статьи / Authors of the article

уровень метастабильного режима; у реально отобранного экземпляра с остаточной асимметрией вероятность появления единицы отклоняется от идеального значения 0.5, что необходимо учитывать при переносе полученных оценок на конкретные образцы. Моделирование выполнено на поведенческом уровне; тепловой шум представлен упрощённой моделью AWGN, не учитывающей окрашенность и зависимость от температуры и напряжения питания. Кроме того, тепловой шум задаётся программным генератором псевдослучайных чисел с фиксированным начальным значением, поэтому полученные статистические результаты в первую очередь подтверждают корректность логики предложенной модели, а не свойства физического источника энтропии. Выборка 10^6 бит достаточна для демонстрации качества, но не для полносертификационных испытаний по всем 15 тестам NIST. Физический прототип на данном этапе отсутствует, что оставляет открытым вопрос о влиянии реальных паразитных эффектов (перекрёстные наводки, нестабильность питания) на качество случайности.

Заключение

В работе исследована возможность использования стандартного JK-триггера в метастабильном режиме в качестве генератора истинно случайных чисел. Предложена поведенческая модель «Весы», описывающая состязание сигналов в Master-ступени через взаимодействие систематической асимметрии задержек Δt_{chip} и теплового шума $\eta(t)$. Показано, что при технологической симметрии ($\Delta t_{\text{chip}} \approx 0$) исход каждого такта определяется исключительно шумом, а выходные биты статистически независимы.

Поведенческое моделирование на выборке 10^6 бит для случая полностью скомпенсированной асимметрии ($\Delta t_{\text{chip}} = 0$) подтвердило высокое качество случайности: смещение составило 0.0004, энтропия Шеннона — 1.0000, минимальная энтропия — 0.9989. Тесты NIST SP 800-22 (Frequency, Block Frequency, Runs) пройдены с P-value от 0.17 до 0.74. Автокорреляционный анализ не выявил значимых зависимостей между битами. Отметим, что перечисленные показатели характеризуют предельно достижимый уровень: у реального отобранного экземпляра с остаточной асимметрией вероятность появления единицы отклоняется от идеального значения, а поскольку тепловой шум моделировался программным генератором псевдослучайных чисел с фиксированным начальным значением, полученные результаты подтверждают в первую очередь корректность логики предложенной модели, а не свойства физического источника энтропии.

Практическая значимость предложенного подхода состоит в том, что ГИСЧ реализуется на стандартной библиотечной ячейке без каких-либо схемных модификаций, что упрощает его интеграцию в ПЛИС и СнК.

Рост числа распределённых информационных систем, платформ на основе блокчейн-технологий и автономных программных агентов значительно повышает требования к качеству используемых криптографических механизмов. Надёжные аппаратные генераторы истинно случайных чисел становятся одним из базовых компонентов подобных систем, поскольку используются при формировании криптографических ключей, одноразовых идентификаторов и других элементов инфраструктуры доверия. По этой причине предложенный подход может представлять практический интерес не только для аппаратной криптографии, но и для перспективных распределённых вычислительных платформ, использующих механизмы децентрализованного доверия [17], [18].

Направления дальнейших исследований включают: реализацию физического прототипа на ПЛИС или заказной микросхеме; исследование влияния температуры и напряжения питания на качество случайности; расширение набора статистических тестов до полной батареи NIST SP 800-22; разработку схемы автоматического поиска симметричных экземпляров триггера на кристалле и компенсации остаточной асимметрии программируемыми элементами задержки.

Конфликт интересов

Не указан.

Рецензия

Борисов А.Н., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань Российская Федерация
DOI: https://doi.org/10.60797/IRJ.2026.173.72.8

Conflict of Interest

None declared.

Review

Borisov A.N., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan Russian Federation
DOI: https://doi.org/10.60797/IRJ.2026.173.72.8

Список литературы / References

1. Шарипов Р.Р. Разработка программно-лабораторного комплекса для изучения кодирования информации методом Хаффмана / Р.Р. Шарипов, Е.Д. Ожмекова, М.Ю. Перухин // Computational Nanotechnology. — 2026. — Т. 13. — № 1. — С. 167–174. — DOI: 10.33693/2313-223X-2026-13-1-167-174.

2. Nguyen Ph.H. A real-time deep learning framework for anomaly detection in data streams using Apache Spark / Ph.H. Nguyen, R.R. Sharipov // Soft Measurements and Computing. — 2026. — Vol. 100. — № 3–4. — P. 97–103. — DOI: 10.36871/26189976.2026.03-4.010.

3. Юсупов Б.З. Разработка стенда для контроля и анализа пороговых извещателей / Б.З. Юсупов // Прикладная электродинамика, фотоника и живые системы — 2024: материалы Международной научно-технической конференции молодых учёных, аспирантов и студентов (Казань, 11–12 апреля 2024 г.) / Казанский национальный исследовательский технический университет им. А.Н. Туполева — КАИ. — Казань: ИП Сагиева А.Р., 2024. — С. 909–910.

4. Юсупов Б.З. Исследование электрических параметров магнитоконтактных извещателей / Б.З. Юсупов // Прикладная электродинамика, фотоника и живые системы — 2024: материалы Международной научно-технической конференции молодых учёных, аспирантов и студентов (Казань, 11–12 апреля 2024 г.) / Казанский национальный исследовательский технический университет им. А.Н. Туполева — КАИ. — Казань: ИП Сагиева А.Р., 2024. — С. 905–906.

 © Авторы статьи / Authors of the article

5. Бондаренко В.В. Блокчейн как инфраструктура доверия для автономных агентов / В.В. Бондаренко, Р.Р. Шарипов, Р.А. Олин // Журнал монетарной экономики и менеджмента. — 2026. — № 7. — С. 28–34. — DOI: 10.26118/2782-4586-2026-28-34.

6. Иванов М.А. Генераторы случайных чисел для криптографии: обзор и классификация / М.А. Иванов, А.В. Ковалёв // Вопросы кибербезопасности. — 2019. — № 5. — С. 2–15.

7. Титце У. Полупроводниковая схемотехника / У. Титце, К. Шенк; пер. с нем. — 12-е изд. — Москва: ДМК Пресс, 2008. — 832 с.

8. Угрюмов Е.П. Цифровая схемотехника / Е.П. Угрюмов. — 3-е изд. — Санкт-Петербург: БХВ-Петербург, 2010. — 816 с.

9. Gassend B. Silicon physical random functions / B. Gassend, D. Clarke, M. van Dijk, S. Devadas // Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02). — Washington: ACM, 2002. — P. 148–160.

10. Holcomb D.E. Power-up SRAM state as an identifying fingerprint and source of true random numbers / D.E. Holcomb, W.P. Burleson, K. Fu // IEEE Transactions on Computers. — 2009. — Vol. 58. — № 9. — P. 1198–1210.

11. Killmann W. A proposal for functionality classes for random number generators: BSI AIS 20/31 / W. Killmann, W. Schindler. — Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2011. — 134 p.

12. Maes R. Physically unclonable functions: a study on the state of the art and future research directions / R. Maes, I. Verbauwhede // Towards Hardware-Intrinsic Security. — Berlin: Springer, 2010. — P. 3–37.

13. Rukhin A. A statistical test suite for random and pseudorandom number generators for cryptographic applications: NIST Special Publication 800-22, Rev. 1a / A. Rukhin, J. Soto, J. Nechvatal [et al.]. — Gaithersburg: National Institute of Standards and Technology, 2010. — 131 p.

14. Suh G.E. Physical unclonable functions for device authentication and secret key generation / G.E. Suh, S. Devadas // Proceedings of the 44th Design Automation Conference (DAC'07). — San Diego: ACM/IEEE, 2007. — P. 9–14.

15. Sunar B. A provably secure true random number generator with built-in tolerance to active attacks / B. Sunar, W.J. Martin, D.R. Stinson // IEEE Transactions on Computers. — 2007. — Vol. 56. — № 1. — P. 109–119.

16. Texas Instruments. SN5476, SN7476 Dual J-K Flip-Flops with Preset and Clear: datasheet SDLS121 / Texas Instruments. — Dallas: Texas Instruments, 1983. — 12 p.

17. Vasyltsov I. Fast digital TRNG based on metastable ring oscillator / I. Vasyltsov, E. Hambardzumyan, Y.-S. Kim, B. Karpinskyy // Cryptographic Hardware and Embedded Systems — CHES 2008: Lecture Notes in Computer Science, Vol. 5154. — Berlin: Springer, 2008. — P. 164–180.

18. Утеев Г. Разработка децентрализованной системы идентификации личности по биометрическим данным с помощью технологии блокчейн и компьютерного зрения / Г. Утеев, Р.Ф. Гибадуллин // Международный научно-исследовательский журнал. — 2024. — № 4 (142). — DOI: 10.23670/IRJ.2024.142.6.

Список литературы на английском языке / References in English

1. Sharipov R.R. Razrabotka programmno-laboratornogo kompleksa dlja izuchenija kodirovanija informacii metodom Hafm ana [Development of a software and laboratory complex for studying information encoding by the Huffman method] / R.R. Sharipov, E.D. Ozhmekova, M.Ju. Peruhin // Computational Nanotechnology [Computational Nanotechnology]. — 2026. — Vol. 13. — № 1. — P. 167–174. — DOI: 10.33693/2313-223X-2026-13-1-167-174. [in Russian]

2. Nguyen Ph.H. A real-time deep learning framework for anomaly detection in data streams using Apache Spark / Ph.H. Nguyen, R.R. Sharipov // Soft Measurements and Computing. — 2026. — Vol. 100. — № 3–4. — P. 97–103. — DOI: 10.36871/26189976.2026.03-4.010.

3. Jusupov B.Z. Razrabotka stenda dlja kontrolja i analiza porogovyh izveshhatelej [Development of a test bench for monitoring and analysis of threshold detectors] / B.Z. Jusupov // Prikladnaja jelektrodinamika, fotonika i zhivye sistemy — 2024: materialy Mezhdunarodnoj nauchno-tehnicheskoj konferencii molodyh uchjonyh, aspirantov i studentov (Kazan', 11–12 aprelja 2024 g.) [Applied Electrodynamics, Photonics and Living Systems — 2024: proceedings of the International Scientific and Technical Conference of Young Scientists, Postgraduates and Students (Kazan, 11–12 April 2024)] / A.N. Tupolev Kazan National Research Technical University — KAI. — Kazan: A.R. Sagieva, individual entrepreneur., 2024. — P. 909–910. [in Russian]

4. Jusupov B.Z. Issledovanie jelektricheskih parametrov magnitokontaktnyh izveshhatelej [Study of the electrical parameters of magnetic contact detectors] / B.Z. Jusupov // Prikladnaja jelektrodinamika, fotonika i zhivye sistemy — 2024: materialy Mezhdunarodnoj nauchno-tehnicheskoj konferencii molodyh uchjonyh, aspirantov i studentov (Kazan', 11–12 aprelja 2024 g.) [Applied Electrodynamics, Photonics and Living Systems — 2024: proceedings of the International Scientific and Technical Conference of Young Scientists, Postgraduates and Students (Kazan, 11–12 April 2024)] / A.N. Tupolev Kazan National Research Technical University — KAI. — Kazan: A.R. Sagieva, individual entrepreneur, 2024. — P. 905–906. [in Russian]

5. Bondarenko V.V. Blokchejn kak infrastruktura doverija dlja avtonomnyh agentov [Blockchain as a trust infrastructure for autonomous agents] / V.V. Bondarenko, R.R. Sharipov, R.A. Olin // Zhurnal monetarnoj jekonomiki i menedzhmenta [Journal of Monetary Economics and Management]. — 2026. — № 7. — P. 28–34. — DOI: 10.26118/2782-4586-2026-28-34. [in Russian]

6. Ivanov M.A. Generatory sluchajnyh chisel dlja kriptografii: obzor i klassifikacija [Random number generators for cryptography: review and classification] / M.A. Ivanov, A.V. Kovaljov // Voprosy kiberbezopasnosti [Cybersecurity Issues]. — 2019. — № 5. — P. 2–15. [in Russian]

7. Titce U. Poluprovodnikovaja shemotehnika [Semiconductor circuit engineering] / U. Titce, K. Shenk. — 12-th ed. — Moscow: DMK Press, 2008. — 832 p. [in Russian]

 © Авторы статьи / Authors of the article

8. Ugrjumov E.P. Cifrovaja shemotehnika [Digital circuit engineering] / E.P. Ugrjumov. — 3-rd ed. — St. Petersburg: BHV-Peterburg, 2010. — 816 p. [in Russian]

9. Gassend B. Silicon physical random functions / B. Gassend, D. Clarke, M. van Dijk, S. Devadas // Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS'02). — Washington: ACM, 2002. — P. 148–160.

10. Holcomb D.E. Power-up SRAM state as an identifying fingerprint and source of true random numbers / D.E. Holcomb, W.P. Burleson, K. Fu // IEEE Transactions on Computers. — 2009. — Vol. 58. — № 9. — P. 1198–1210.

11. Killmann W. A proposal for functionality classes for random number generators: BSI AIS 20/31 / W. Killmann, W. Schindler. — Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2011. — 134 p.

12. Maes R. Physically unclonable functions: a study on the state of the art and future research directions / R. Maes, I. Verbauwhede // Towards Hardware-Intrinsic Security. — Berlin: Springer, 2010. — P. 3–37.

13. Rukhin A. A statistical test suite for random and pseudorandom number generators for cryptographic applications: NIST Special Publication 800-22, Rev. 1a / A. Rukhin, J. Soto, J. Nechvatal [et al.]. — Gaithersburg: National Institute of Standards and Technology, 2010. — 131 p.

14. Suh G.E. Physical unclonable functions for device authentication and secret key generation / G.E. Suh, S. Devadas // Proceedings of the 44th Design Automation Conference (DAC'07). — San Diego: ACM/IEEE, 2007. — P. 9–14.

15. Sunar B. A provably secure true random number generator with built-in tolerance to active attacks / B. Sunar, W.J. Martin, D.R. Stinson // IEEE Transactions on Computers. — 2007. — Vol. 56. — № 1. — P. 109–119.

16. Texas Instruments. SN5476, SN7476 Dual J-K Flip-Flops with Preset and Clear: datasheet SDLS121 / Texas Instruments. — Dallas: Texas Instruments, 1983. — 12 p.

17. Vasyltsov I. Fast digital TRNG based on metastable ring oscillator / I. Vasyltsov, E. Hambardzumyan, Y.-S. Kim, B. Karpinskyy // Cryptographic Hardware and Embedded Systems — CHES 2008: Lecture Notes in Computer Science, Vol. 5154. — Berlin: Springer, 2008. — P. 164–180.

18. Uteev G. Razrabotka decentralizovannoj sistemy identifikacii lichnosti po biometricheskim dannym s pomoshh'ju tehnologii blokchejn i komp'juternogo zrenija [Development of a decentralized personal identification system based on biometric data using blockchain technology and computer vision] / G. Uteev, R.F. Gibadullin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Research Journal]. — 2024. — № 4 (142). — DOI: 10.23670/IRJ.2024.142.6. [in Russian]