№6/2026



ADPI
Ilmiy xabarnomasi

ПРИМЕНЕНИЕ ЭНТРОПИИ ШЕННОНА И ДИВЕРГЕНЦИИ КУЛЬБАКА–ЛЕЙБЛЕРА В ЗАДАЧАХ КРИПТОАНАЛИЗА ЛЕГКОВЕСНЫХ БЛОЧНЫХ ШИФРОВ

Ортиков Муроджон Сойибжонович
Андижанской государственный технический институт

Annotatsiya.
Maqolada Shennon entropiyasi va Kulbak–Leybler divergensiyasining PRESENT-80, GIFT-64-128, SIMON-64/128 va SPECK-64/128 yengil blokli shifrlarining statistik xossalarini baholash imkoniyatlari tadqiq etilgan. Tajriba har bir raundlar soni uchun past entropiyali kirishning (hisoblagichning) 65 536 bloki ustida χ^2 mezoni, NIST SP 800-22 testlari va qat'iy ko'chkisimon mezoni (SAC) yordamida o'tkazilgan. To'liq raundli algoritmlar statistik jihatdan tasodifiy manbadan farqlanmaydi: 7,99964–7,99973 bit baytli entropiya ushbu tanlanma hajmi uchun nazariy kutilgan qiymatga mos keladi. Statistik tasodifiylik uchun zarur raundlar soni mos ravishda 10, 7, 12 va 7 ni, ya'ni to'liq raundlar sonining 25–32 % ini tashkil etdi. Entropiya o'lchovlari to'liq bo'lmagan diffuziyani aniqlay olmasligi ko'rsatilgan: 3 raundli SPECK-64/128 SAC chetlanishi 0,5 bo'lganda ham entropiya testlaridan o'tadi. Entropiya o'lchovlarini ko'chkisimon mezoni bilan birgalikda qo'llash zarur degan xulosa qilingan.

Kalit so'zlar:
yengil kriptografiya, blokli shifr, Shennon entropiyasi, Kulbak–Leybler divergensiyasi, lavina effekti, qat'iy lavina mezoni, PRESENT, GIFT, SIMON, SPECK.

Аннотация.
Исследованы возможности энтропии Шеннона и дивергенции Кульбака–Лейблера для оценки статистических свойств легковесных блочных шифров PRESENT-80, GIFT-64-128, SIMON-64/128 и SPECK-64/128. Эксперимент выполнен на 65 536 блоках низкоэнтропийного входа (счётчика) для каждого числа раундов с применением критерия χ^2, тестов NIST SP 800-22 и лавинного критерия SAC. Полнораундовые алгоритмы статистически неотличимы от случайного источника: байтовая энтропия 7,99964–7,99973 бита совпадает с теоретическим ожиданием для данного объёма выборки. Число раундов статистической случайности составило 10, 7, 12 и 7 соответственно, то есть 25–32 % от полного числа раундов. Показано, что энтропийные меры не выявляют неполную диффузию: SPECK-64/128 после 3 раундов проходит энтропийные тесты при отклонении SAC 0,5. Сделан вывод о необходимости совместного применения энтропийных мер и лавинного критерия.

Ключевые слова:
легковесная криптография, блочный шифр, энтропия Шеннона, дивергенция Кульбака–Лейблера, лавинный эффект, критерий SAC, PRESENT, GIFT, SIMON, SPECK.

Abstract.
The paper studies the capability of Shannon entropy and Kullback–Leibler divergence to assess the statistical properties of the lightweight block ciphers PRESENT-80, GIFT-64-128, SIMON-64/128 and SPECK-64/128. The experiment uses 65,536 blocks of low-entropy (counter) input for every number of rounds, together with the χ^2 test, NIST SP 800-22 tests and the strict avalanche criterion (SAC). The full-round ciphers are statistically indistinguishable from a random source: byte entropy of 7.99964–7.99973 bits matches the theoretical expectation for this sample size. The number of rounds needed for statistical randomness is 10, 7, 12 and 7 respectively, or 25–32 % of the full round count. Entropy measures fail to detect incomplete diffusion: 3-round SPECK-64/128 passes entropy tests while its SAC deviation equals 0.5. Entropy measures should therefore be used together with the avalanche criterion.

Keywords:
lightweight cryptography, block cipher, Shannon entropy, Kullback–Leibler divergence, avalanche effect, strict avalanche criterion, PRESENT, GIFT, SIMON, SPECK.

1. Введение. Сегодня умные гаджеты, датчики и встроенные системы окружают нас повсюду — от умного дома до медицины. Большинство этих устройств совсем крошечные, и у них нет мощных процессоров. Если попытаться установить на них обычную компьютерную защиту, они просто «зависнут», моментально разрядят батарейку или им банально не хватит памяти. Ответом на эту проблему стала легковесная криптография, в рамках которой разработаны блочные шифры PRESENT [5], GIFT [6], SIMON и SPECK [7]. Национальный институт стандартов и технологий США по итогам конкурса легковесной криптографии выбрал в 2023 году семейство ASCON и в 2025 году утвердил его в качестве стандарта [12], что подтверждает практическую значимость данного направления. Общие вопросы проектирования и анализа блочных шифров рассмотрены в монографиях [8–10, 14, 15].

ISSN 2181-4309

Оценка стойкости новых и модифицированных легковесных шифров традиционно опирается на линейный [1] и дифференциальный [2] криптоанализ. Эти методы требуют глубокого анализа структуры алгоритма и значительных вычислительных затрат. На ранних этапах проектирования востребованы более простые инструменты, позволяющие быстро выявить грубые статистические дефекты преобразования. Таким инструментом могут служить информационно-теоретические меры — энтропия Шеннона [3, 4] и дивергенция Кульбака–Лейблера — в сочетании со статистическими критериями случайности [11].

Вместе с тем при использовании статистических тестов часто допускается методическая ошибка: на вход шифра подаются случайные открытые тексты. Любая биекция переводит равномерное распределение в равномерное, поэтому высокие значения энтропии на выходе в этом случае ничего не говорят о качестве шифра. Корректная постановка требует структурированных входных данных с низкой энтропией и анализа шифров с уменьшенным числом раундов.

Цель работы — экспериментально оценить возможности энтропийных мер и статистических критериев для выявления неслучайности выходных данных легковесных блочных шифров.

Для достижения цели решаются следующие **задачи**:

1. Программно реализовать алгоритмы PRESENT-80, GIFT-64-128, SIMON-64/128 и SPECK-64/128 с проверкой по эталонным тестовым векторам.
2. Сформировать случайную и структурированную (низкоэнтропийную) выборки открытых текстов.
3. Рассчитать энтропию Шеннона, дивергенцию Кульбака–Лейблера, критерий χ^2 и тесты NIST SP 800-22 для выходных данных полнораундовых шифров.
4. Исследовать лавинный эффект и зависимость статистических показателей от числа раундов.
5. Сравнить алгоритмы по числу раундов, необходимому для достижения статистической неотличимости от случайной последовательности.

2. Теоретические основы

Энтропия Шеннона. Пусть выходные данные шифра рассматриваются как последовательность символов алфавита из k значений, где p_i — относительная частота i-го символа. Энтропия Шеннона [3] определяется выражением

$$H(X) = -\sum_{i=1}^{k} p_i \log_2 p_i$$

Для битового алфавита (k = 2) максимальное значение H = 1 бит, для байтового (k = 256) — 8 бит. Близость энтропии к максимуму означает равномерность распределения символов. Шеннон показал [4], что совершенная секретность достигается тогда, когда шифртекст не несёт информации об открытом тексте.

Дивергенция Кульбака–Лейблера [13] измеряет отклонение эмпирического распределения P от равномерного распределения U, где $u_i = 1/k$:

$$D_{KL}(P \parallel U) = \sum_{i=1}^{k} p_i \log_2 \frac{p_i}{u_i} = \log_2 k - H(X)$$

ISSN 2181-4309

Из выражения следует, что DKL и H(X) для равномерного эталона несут одну и ту же информацию: DKL равна дефициту энтропии. Поэтому в работе DKL используется как удобная мера отклонения, а не как независимый критерий.

Критерий χ^2 Пирсона проверяет гипотезу H0 о равномерности распределения:

$$\chi^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$$

где O_i — наблюдаемое, $E_i = N/k$ — ожидаемое число появлений символа, N — объём выборки. Статистика имеет k − 1 степеней свободы. Гипотеза отвергается при p-значении меньше уровня значимости α = 0,01, принятого в NIST SP 800-22 [11].

Важная оговорка о конечной выборке. Эмпирическая энтропия смещена вниз: даже для идеально случайного источника её оценка меньше максимума. По приближению Миллера–Мэдоу [16] ожидаемый дефицит составляет

$$E[\Delta H] \approx \frac{k-1}{2N \ln 2}$$

Например, для 80 000 байтов (k = 256) ожидаемая оценка энтропии равна примерно 7,9977 бит, а не 8. Без учёта этого смещения малые отклонения от максимума ошибочно интерпретируются как дефект шифра.

Лавинный эффект. Для открытого текста P и текста P′, отличающегося одним битом, вычисляется доля изменившихся битов шифртекста:

$$A = \frac{HW\left(E_K(P) \oplus E_K(P')\right)}{n} \times 100\%$$

где HW — вес Хэмминга, n = 64 — размер блока. Для хорошего шифра A ≈ 50 %. Более строгий критерий лавинного эффекта (SAC) [17] требует, чтобы каждый выходной бит менялся с вероятностью 0,5 при изменении любого входного бита. Мерой нарушения SAC служит максимальное отклонение элементов матрицы вероятностей 64 × 64 от значения 0,5.

3. Методика вычислительного эксперимента

Исследуемые алгоритмы. Параметры алгоритмов приведены в таблице 1.

Таблица 1 – Параметры исследуемых алгоритмов

Алгоритм	Структура	Блок, бит	Ключ, бит	Число раундов	Источник
PRESENT-80	SPN, 4-битовый S-блок, битовая перестановка	64	80	31	[5]
GIFT-64-128	SPN, 4-битовый S-блок, битовая перестановка	64	128	28	[6]
SIMON-64/128	Фейстель, AND-ROT-XOR	64	128	44	[7]
SPECK-64/128	ARX (сложение, сдвиг, XOR)	64	128	27	[7]

Программная реализация. Алгоритмы реализованы авторами на языке Python 3.13 с векторизацией средствами NumPy 2.5. Реализация допускает произвольное число раундов r, что необходимо для анализа шифров с уменьшенным числом раундов. Корректность проверена по эталонным тестовым векторам разработчиков: по два

вектора для PRESENT-80 и GIFT-64-128, по одному для SIMON-64/128 и SPECK-64/128. Все шесть векторов совпали.

Входные выборки. Использовались две выборки по N = 65 536 блоков (4 194 304 бита):

• выборка R — случайные 64-битные открытые тексты от генератора PCG64 (seed = 2026);

• выборка C — счётчик 0, 1, 2, …, 65 535 (низкоэнтропийный вход: 48 старших битов каждого блока равны нулю).

Выборка C является основной. Байтовая энтропия самого счётчика составляет 2,80 бита из 8, доля единиц — 0,125. Если шифр после r раундов выдаёт статистически случайный выход из такого входа, это говорит о реальном перемешивании. Выборка R используется только для сравнения: для неё равномерный выход ожидается при любом числе раундов.

Ключи. Для каждого алгоритма использовался один случайный ключ, сгенерированный тем же генератором и фиксированный на всё время эксперимента.

Оцениваемые показатели. Для каждой выходной последовательности рассчитывались:

1. Доля единичных битов, битовая энтропия и битовая DKL.
2. Байтовая энтропия H_8 (алфавит из 256 символов, 524 288 байтов) и байтовая $DKL = 8 - H_8$.
3. Критерий χ^2 по байтам (255 степеней свободы).
4. Тесты NIST SP 800-22 [11]: частотный (monobit), блочный частотный (M = 128) и тест серий (runs).

Критерий χ^2 по битам с одной степенью свободы математически эквивалентен частотному тесту NIST, поэтому отдельно не приводится. Уровень значимости $\alpha = 0{,}01$.

Лавинный эффект. Для 4 000 случайных открытых текстов поочерёдно инвертировался каждый из 64 битов (256 000 пар). Рассчитывались среднее, минимальное и максимальное значение A, а также максимальное отклонение матрицы SAC от 0,5.

Для корректного сравнения нужен порог: какое отклонение SAC даёт идеально случайная функция при той же выборке. Он был получен моделированием (20 повторов): среднее максимальное отклонение — 0,030, наибольшее — 0,040. Значения SAC ниже 0,040 считались неотличимыми от случайных.

Анализ по раундам. Для выборки C и каждого r от 1 до полного числа раундов рассчитывались все перечисленные показатели. Число раундов статистической случайности r* определялось как первый раунд, начиная с которого одновременно выполняются три условия: $p(\chi^2) > 0{,}01$, отклонение SAC < 0,040 и среднее A в пределах 50 ± 0,5 %.

Полный цикл расчётов занимает около 67 секунд на одном ядре процессора x86_64 под ОС Linux. Исходный код и все полученные данные приложены к статье.

4. Результаты исследования

4.1. Полнораундовые алгоритмы

Все четыре полнораундовых алгоритма дают выход, статистически неотличимый от случайного, на обеих выборках. Результаты для основной выборки C приведены в таблице 2.

ISSN 2181-4309

Таблица 2 – Статистические показатели полнораундовых алгоритмов (выборка C, N = 65 536 блоков)

Алгоритм	Доля единиц	H_8, бит	DKL_8, бит	χ^2 (255 ст. св.)	$p(\chi^2)$	p monobit	p block freq.	p runs
Вход (счётчик)	0,1250	2,80051	5,19949	75 202 560	$< 10^{-300}$	$< 10^{-300}$	$< 10^{-300}$	$< 10^{-300}$
PRESENT-80	0,5002	7,999967	0,00033	241,1	0,726	0,455	0,440	0,960
GIFT-64-128	0,4999	7,999964	0,00036	260,8	0,388	0,648	0,768	0,419
SIMON-64/128	0,5000	7,999966	0,00034	245,9	0,647	0,871	0,066	0,093
SPECK-64/128	0,5002	7,999973	0,00027	196,5	0,997	0,468	0,873	0,192

На выборке R картина аналогична: байтовая энтропия составила от 7,99960 до 7,99966 бита, все $p(\chi^2) > 0,05$.

Важно правильно интерпретировать значения H_8. Они не равны 8 не из-за дефектов шифров. По формуле Миллера–Мэдоу для 524 288 байтов ожидаемая оценка энтропии идеально случайного источника равна 7,99965 бита. Полученные значения 7,99964–7,99973 точно совпадают с этим ожиданием. Различия между алгоритмами в пятом знаке после запятой — это статистический шум, и ранжировать по ним алгоритмы некорректно.

Из 32 проверок (4 алгоритма × 2 выборки × 4 теста) гипотеза случайности отвергнута один раз: частотный тест для SIMON-64/128 на выборке R, $p = 0,004$. При $\alpha = 0,01$ ожидаемое число ложных отклонений составляет 0,32, поэтому единичный случай согласуется со случайностью. На выборке C тот же алгоритм проходит этот тест с $p = 0,871$.

Лавинный эффект полнораундовых алгоритмов также идеален (таблица 3). Стандартное отклонение A теоретически равно $100 \cdot 0,5 / \sqrt{64} = 6,25$ %, что совпадает с полученными значениями.

Таблица 3 – Лавинный эффект полнораундовых алгоритмов (256 000 пар текстов)

Алгоритм	Среднее A, %	СКО A, %	Мин. A, %	Макс. A, %	Макс. отклонение SAC
PRESENT-80	49,99	6,26	21,88	78,12	0,0275
GIFT-64-128	50,00	6,25	21,88	78,12	0,0290
SIMON-64/128	50,01	6,25	20,31	78,12	0,0298
SPECK-64/128	50,00	6,24	21,88	78,12	0,0285
Случайная функция (модель)	50,00	6,25	—	—	0,030 (макс. 0,040)

ISSN 2181-4309

4.2. Алгоритмы с уменьшенным числом раундов

Основные различия между алгоритмами проявляются на малом числе раундов. На рисунке 1 показано, как убывает байтовая KL-дивергенция при обработке счётчика.

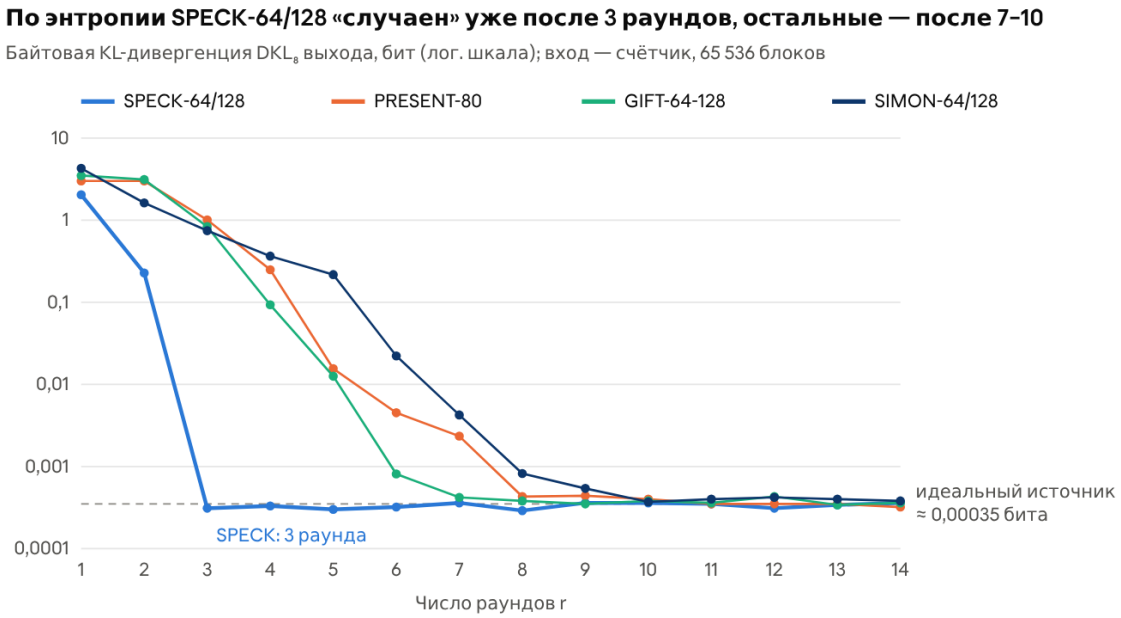


Рисунок 1 – Байтовая KL-дивергенция выхода в зависимости от числа раундов (выборка C, раунды 1–14). Расчёт авторов, results.json

На рисунке 2 для тех же шифров показано отклонение SAC.

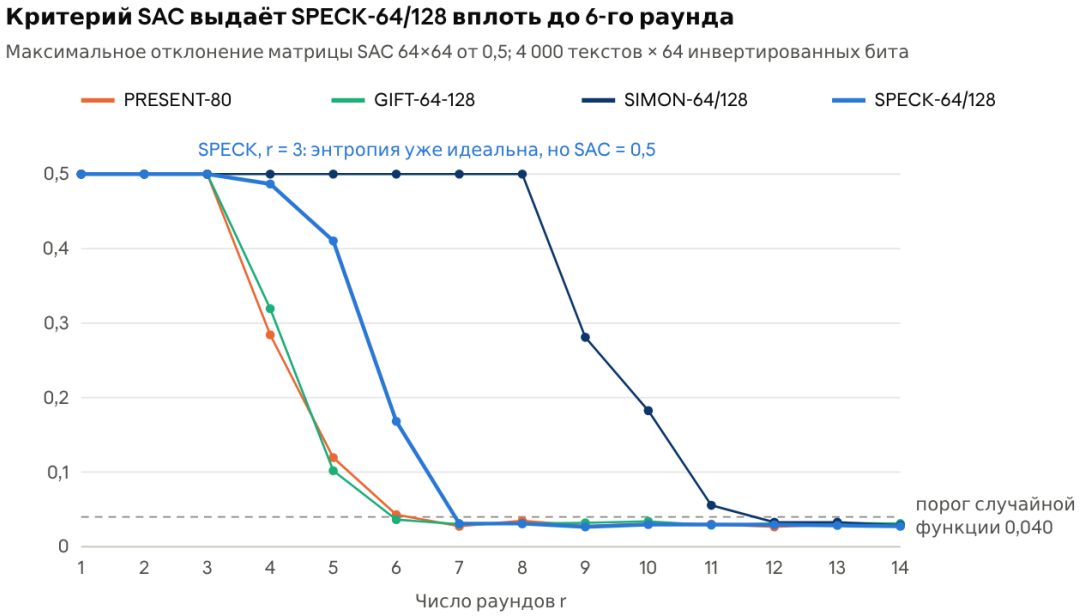


Рисунок 2 – Максимальное отклонение SAC в зависимости от числа раундов (раунды 1–14). Расчёт авторов, results.json

Сопоставление рисунков даёт главный результат работы. Энтропийные меры и SAC приходят к уровню случайности на разных раундах, и для SPECK-64/128 этот разрыв

максимален. Уже после 3 раундов его выход проходит байтовый χ^2 ($p = 0{,}924$) и имеет $DKL_8 = 0{,}00031$ бита, что соответствует идеальному источнику. При этом средний лавинный эффект равен лишь 31,8 %, а отклонение SAC — 0,5: часть выходных битов вообще не зависит от некоторых входных. Энтропийный анализ этот дефект не обнаруживает.

Число раундов статистической случайности r* по всем трём критериям приведено в таблице 4.

Таблица 4 – Число раундов, необходимое для статистической случайности (выборка C)

Алгоритм	**Первый раунд $p(\chi^2) > 0{,}01$**	**Первый раунд SAC < 0,040**	**r***	**Полное число раундов**	**r* / полное, %**
PRESENT-80	10	7	10	31	32
GIFT-64-128	7	6	7	28	25
SIMON-64/128	10	12	12	44	27
SPECK-64/128	3	7	7	27	26

После r* все критерии выполняются во всех последующих раундах за двумя исключениями: GIFT-64-128 на 12-м раунде ($p = 0{,}009$) и SIMON-64/128 на 21-м раунде ($p = 0{,}002$). При 98 таких проверках на уровне $\alpha = 0{,}01$ ожидается около одного ложного отклонения, поэтому эти случаи следует считать статистическими флуктуациями.

Наименьшее абсолютное число раундов до статистической случайности показали GIFT-64-128 и SPECK-64/128 — по 7 раундов. У PRESENT-80 случайность по байтовому χ^2 наступает позже, чем по SAC: после 7 раундов диффузия уже полная, но распределение байтов ещё смещено ($p(\chi^2) = 6 \cdot 10^{-212}$). SIMON-64/128 требует 12 раундов, однако по доле от полного числа раундов (27 %) он не уступает остальным.

5. Обсуждение

Ограниченность энтропийных мер. Энтропия Шеннона и DKL оценивают только частоты символов, но не зависимость выхода от входа. Пример SPECK-64/128 показывает, что выход может иметь идеальное распределение байтов при неполной диффузии. Поэтому энтропийный анализ выявляет лишь грубые дефекты и должен дополняться критериями, учитывающими связь «вход — выход», прежде всего SAC.

Методическая ошибка случайного входа. Шифр с фиксированным ключом является перестановкой множества 64-битных блоков. Перестановка случайной выборки остаётся случайной выборкой, поэтому тесты на выборке R проходят при любом числе раундов, даже при r = 1. Содержательные выводы о качестве

ISSN 2181-4309

преобразования можно делать только на структурированных входных данных, как выборка C.

Статистическая случайность и криптографическая стойкость. Все полнораундовые алгоритмы прошли все тесты, а различия между ними лежат в пределах статистической погрешности. Статистические тесты не позволяют ранжировать стандартные полнораундовые шифры по стойкости. Кроме того, r* составляет 25–32 % от полного числа раундов, тогда как известные атаки линейного и дифференциального криптоанализа [1, 2] охватывают существенно большее число раундов. Следовательно, статистическая случайность — необходимое, но не достаточное условие стойкости.

Ограничения исследования. Эксперимент проведён для одного ключа на алгоритм и одного типа структурированного входа. Результаты для отдельных раундов вблизи r* могут зависеть от ключа. Для повышения надёжности выводов целесообразно повторить расчёты для нескольких ключей и других низкоэнтропийных входов (например, текстов с малым весом Хэмминга).

Научная новизна

1. Экспериментально показано, что энтропия Шеннона и дивергенция Кульбака–Лейблера неспособны обнаружить неполную диффузию в легковесном ARX-шифре: SPECK-64/128 после 3 раундов проходит энтропийные тесты при отклонении SAC 0,5.
2. Предложена методика пораундовой оценки, сочетающая низкоэнтропийную входную выборку, байтовую энтропию с поправкой на конечный объём выборки и критерий SAC с порогом, полученным моделированием случайной функции.
3. В единых условиях эксперимента получены значения числа раундов статистической случайности r* для PRESENT-80, GIFT-64-128, SIMON-64/128 и SPECK-64/128.

Практическая значимость

Предложенная методика позволяет на этапе проектирования или модификации легковесного шифра за минуты вычислений определить минимальное число раундов, при котором выход становится статистически неотличимым от случайного. Методика применима для проверки корректности программных и аппаратных реализаций, в учебном процессе по дисциплинам защиты информации, а также для предварительного отбора вариантов алгоритмов перед трудоёмким линейным и дифференциальным криптоанализом.

6. Заключение

В работе выполнено экспериментальное исследование статистических свойств легковесных блочных шифров PRESENT-80, GIFT-64-128, SIMON-64/128 и SPECK-64/128 с применением энтропии Шеннона, дивергенции Кульбака–Лейблера, критерия χ^2,

тестов NIST SP 800-22 и лавинного критерия. Реализации алгоритмов проверены по эталонным тестовым векторам.

Получены следующие основные результаты:

1. Все полнораундовые алгоритмы формируют выход, статистически неотличимый от случайного. Байтовая энтропия 7,99964–7,99973 бита совпадает с ожидаемым значением 7,99965 для идеального источника при данном объёме выборки, средний лавинный эффект равен 50,0 %.
2. Различия показателей полнораундовых алгоритмов находятся в пределах статистической погрешности и не могут служить основанием для их ранжирования по стойкости.
3. Число раундов статистической случайности r* составляет 10 для PRESENT-80, 7 для GIFT-64-128, 12 для SIMON-64/128 и 7 для SPECK-64/128, то есть 25–32 % от полного числа раундов.
4. Энтропийные меры не обнаруживают неполную диффузию: SPECK-64/128 после 3 раундов проходит энтропийные тесты при среднем лавинном эффекте 31,8 % и отклонении SAC 0,5.
5. Тестирование шифров на случайных открытых текстах не информативно; корректная оценка требует низкоэнтропийных входных данных.

Таким образом, энтропийный анализ целесообразно использовать как быстрый первичный фильтр при проектировании легковесных шифров, но только совместно с лавинным критерием и с поправкой на объём выборки. Он не заменяет линейный и дифференциальный криптоанализ. Направления дальнейших исследований: повторение эксперимента для множества ключей, применение условной энтропии и взаимной информации между входом и выходом, расширение набора алгоритмов финалистами конкурса NIST, в том числе ASCON.

Список литературы:

1. Matsui M. Linear Cryptanalysis Method for DES Cipher // Advances in Cryptology – EUROCRYPT'93. – Berlin: Springer, 1994. – P. 386–397.
2. Biham E., Shamir A. Differential Cryptanalysis of the Data Encryption Standard. – New York: Springer, 1993. – 188 p.
3. Shannon C. E. A Mathematical Theory of Communication // Bell System Technical Journal. – 1948. – Vol. 27, No. 3. – P. 379–423.
4. Shannon C. E. Communication Theory of Secrecy Systems // Bell System Technical Journal. – 1949. – Vol. 28, No. 4. – P. 656–715.
5. Bogdanov A., Knudsen L. R., Leander G. et al. PRESENT: An Ultra-Lightweight Block Cipher // Cryptographic Hardware and Embedded Systems – CHES 2007. – Berlin: Springer, 2007. – P. 450–466.
6. Banik S., Pandey S. K., Peyrin T. et al. GIFT: A Small Present // Cryptographic Hardware and Embedded Systems – CHES 2017. – Cham: Springer, 2017. – P. 321–345.
7. Beaulieu R., Shors D., Smith J. et al. The SIMON and SPECK Lightweight Block Ciphers // Proceedings of the 52nd Annual Design Automation Conference (DAC'15). – New York: ACM, 2015. – P. 1–6.

8. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. – Boca Raton: CRC Press, 1996. – 816 p.
9. Stallings W. Cryptography and Network Security: Principles and Practice. – 8th ed. – Hoboken: Pearson, 2020. – 800 p.
10. Paar C., Pelzl J. Understanding Cryptography. – Berlin: Springer, 2010. – 372 p.
11. Bassham L., Rukhin A., Soto J. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications: NIST SP 800-22 Rev. 1a. – Gaithersburg: NIST, 2010.
12. Ascon-Based Lightweight Cryptography Standards for Constrained Devices: NIST SP 800-232. – Gaithersburg: NIST, 2025.
13. Kullback S., Leibler R. A. On Information and Sufficiency // The Annals of Mathematical Statistics. – 1951. – Vol. 22, No. 1. – P. 79–86.
14. Katz J., Lindell Y. Introduction to Modern Cryptography. – 3rd ed. – Boca Raton: CRC Press, 2020. – 648 p.
15. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C. – 20th anniversary ed. – Indianapolis: Wiley, 2015. – 784 p.
16. Miller G. Note on the Bias of Information Estimates // Information Theory in Psychology: Problems and Methods. – Glencoe: Free Press, 1955. – P. 95–100.
17. Webster A. F., Tavares S. E. On the Design of S-Boxes // Advances in Cryptology – CRYPTO'85. – Berlin: Springer, 1986. – P. 523–534.

MUNDARIJA

G'aniyev Abduqahhor Gadoyevich
LIRIK TAFAKKURNI INSONNING SUN'IY INTELLEKTDAN USTUNLIGINI TA'MINLASHDAGI O'RNI 314 318

Uzaqova Noilaxon Ma'ribjon qizi
"ESHITISHIDA NUQSONI BO'LGAN O'QUVCHILAR TA'LIM TARBIYASIDA INKLYUZIV YONDASHUVNING PEDAGOGIK-PSIXOLOGIK SAMARADORLIGINI BAHOLASH" 319 322

Mamasodiqova Saidaxon Soyibjon qizi
RAQAMLI PEDAGOGIKADA STEAM YONDASHUVI ASOSIDA TALABALARNING AXBOROT BILAN ISHLASH KOMPETENTLIGINI RIVOJLANTIRISH 323 332

Abduqodirova Patmaxon Tursunboyevna
MUAMMOLI VA LOYIHA ASOSIDA O'QITISH TEXNOLOGIYALARINI POLIPARADIGMAL METODIKAGA INTEGRATSIYALASH 333 337

Abduqodirova P.T., Xojiyev D.B.
SUN'IY INTELLEKT VA RAQAMLI TA'LIM TEXNOLOGIYALARI ASOSIDA BO'LAJAK INFORMATIKA O'QITUVCHILARINING INTELLEKTUAL QOBILIYATLARINI RIVOJLANTIRISH METODIKASI 338 344

Yunusov Ismonali Kodirovich
MAKTABGACHA TA'LIM TASHKILOTIGA MOSLASHISH DAVRINI YENGILLASHTIRISHNING PEDAGOGIK SHART-SHAROITLARI VA BOSQICHMA-BOSQICH QABUL QILISH ALGORITMI 345 353

Djurayeva Feruzaxon Abdumuxtarovna
VIRTUAL LABORATORIYALAR ASOSIDA ILMIY-TADQIQOT KOMPETENSIYASINI RIVOJLANTIRISH JARAYONINING METODIK JIHATLARI 354 360

Ортиков Муроджон Сойибжонович
ПРИМЕНЕНИЕ ЭНТРОПИИ ШЕННОНА И ДИВЕРГЕНЦИИ КУЛЬБАКА–ЛЕЙБЛЕРА В ЗАДАЧАХ КРИПТОАНАЛИЗА ЛЕГКОВЕСНЫХ БЛОЧНЫХ ШИФРОВ 361 370

O'rinboyev Muxammadzoxir Iqboljon o'g'li
O'QUVCHILARNING FIZIKA FANIGA BO'LGAN QIZIQISH DARAJASINI O'RGANISH VA METAKOGNITIV FAOLIYATLARINI FAOLLASHTIRISH 371 379

Ergashev Murodbek Ikromovich
ADAPTIV YONDASHUV ASOSIDA BO'LAJAK MUSIQA O'QITUVCHILARINING KREATIV KOMPETENTLIGINI TAKOMILLASHTIRISH ZARURATI 380 385

