МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.23

МАТРИЧНАЯ ФОРМУЛА ДЛЯ РАСПРЕДЕЛЕНИЯ ВЫХОДА БЛОЧНОЙ СХЕМЫ ШИФРОВАНИЯ И СТАТИСТИЧЕСКИЙ КРИТЕРИЙ НА ЕЁ ОСНОВЕ

О. В. Денисов, Р. А. Былина

ООО «Центр сертификационных исследований», г. Москва, Россия

Рассматривается произвольная блочная итеративная схема шифрования со случайными независимыми двоичными входными и ключевыми векторами. С помощью псевдобулевого линейного представления итерационной вектор-функции получена матричная формула для спектра распределения выхода. На основе формулы построен статистический критерий проверки гипотезы о том, что наблюдаемые двоичные векторы получены как выход схемы, против гипотезы о равномерности их распределения; рассчитаны асимптотические вероятности ошибок. Проведено экспериментальное сравнение критерия с тестом «стопка книг» (а также с его предлагаемой модификацией) при построении атаки различения на модели блочной шифрсистемы PRESENT с длиной блока 12 битов и числом раундов $R \leqslant 10$.

Ключевые слова: *двоичная вектор-функция, блочная итеративная схема шифрования, спектр распределения, атака различения, тест «стопка книг».*

DOI 10.17223/20710410/32/3

MATRIX FORMULA FOR THE SPECTRUM OF OUTPUT DISTRIBUTION OF BLOCK CIPHER SCHEME AND STATISTICAL CRITERION BASED ON THIS FORMULA

O. V. Denisov, R. A. Bylina

Certification Research Center, Moscow, Russia

E-mail: denisovOleg@yandex.ru, bopobey@rambler.ru

Arbitrary block iterative cipher scheme with random independent binary input and output vectors is considered. A matrix formula for the spectrum of the scheme output distribution is obtained by means of the pseudo-Boolean linear representation of the iterative vector-function. Based on this formula, a statistical criterion of the hypothesis testing that binary vectors are obtained as an output of the scheme against the hypothesis of their uniform distribution is given. Asymptotic type I and type II errors are calculated. An experimental comparison of the criterion with the "Bookstack" test (and its proposed modification) is done during the construction of a distinguishing attack on the mini-models of the block cipher PRESENT (with block size 12 bits and the number of rounds $R \leqslant 10$).

Keywords: *binary vector-function, block iterative cipher scheme, spectrum of distribution, distinguishing attack, the "Bookstack" test.*

Введение

Пусть $(\mathbb{Z}_2, \oplus)$ — группа вычетов по модулю 2, $f = (f_1, \ldots, f_m) : \mathbb{Z}_2^{m+n} \to \mathbb{Z}_2^m$ — двоичная вектор-функция. Рассмотрим блочную схему, в которой из начального двоичного вектора $x = y(0) \in \mathbb{Z}_2^m$ размерности m и двоичных ключевых векторов $k(1), \ldots, k(R) \in \mathbb{Z}_2^n$ размерности n образуется последовательность

$$y(t) = f\left(y(t-1), k(t)\right) \in \mathbb{Z}_2^m, \quad 1 \leqslant t \leqslant R, \tag{1}$$

где R — количество итераций (раундов). Такие схемы могут быть частью блочной шифрсистемы, алгоритма хеширования или выработки псевдослучайной последовательности.

Будем изучать вероятностную модель, в которой

$$x, k(1), \ldots, k(R) \text{ — независимые случайные векторы} \tag{2}$$

и их распределения (в общем случае произвольные) известны. Требуется: 1) найти распределение выхода схемы $y = y(R)$; 2) в случае неравномерного распределения y построить *атаку различения* на схему (1), т. е. критерий для проверки по одинаково распределённым наблюдениям

$$\xi^{(1)}, \ldots, \xi^{(N)} \text{ — независимые случайные векторы, } \xi^{(i)} \sim \xi,\ 1 \leqslant i \leqslant N, \tag{3}$$

простой гипотезы о равномерности их распределения $H_1 : \xi \sim U(\mathbb{Z}_2^m)$ против простой гипотезы $H_2 : \xi \sim y$ о том, что они имеют распределение выходных блоков схемы.

Далее в п. 1 на основе матричного действительнозначного представления функции f получена формула: спектр распределения y представлен произведением спектра распределения x и матриц, соответствующих средним значениям матриц случайных раундовых преобразований. Она позволяет при росте R и фиксированном m вычислять распределение y с временной сложностью, линейно зависящей от R, в то время как общее число 2^{nR} наборов, составленных из раундовых ключей, растет экспоненциально.

В п. 2 с помощью формулы построен критерий проверки гипотез, имеющий заданный асимптотический размер (вероятность ошибки 1-го рода). Получены оценки объёма материала N, при котором вероятность ошибки 2-го рода асимптотически не превосходит заданного значения.

Атаки различения, построенные на базе критерия в рассматриваемых условиях, учитывают внутреннее строение шифрсистемы и распределение входных блоков. Это является большим потенциальным преимуществом критерия по сравнению с универсальными статистическими критериями (тестами). Кроме того, представляется сложной задачей теоретический расчёт вероятностей ошибок универсальных (и специальных) тестов при гипотезе о том, что наблюдаются выходные блоки шифрсистемы. Авторам известны лишь нестрогие оценки таких вероятностей, полученные при эвристических предположениях.

Для экспериментов выбраны оригинальные мини-модели [1] с длиной блока $m = 8, 12$ известной легковесной шифрсистемы PRESENT, в которых алгоритм развёртывания ключа шифрования был заменён случайным неравновероятным выбором раундовых ключей, число раундов $R \leqslant 10$. В п. 3 излагается методика и результаты проведения атак различения, построенных на основе нашего критерия, а также на основе универсального теста «стопка книг» и предложенной его модификации.

1. Матричные формулы

1.1. Линейное представление двоичного отображения

Для булевых функций $g : \mathbb{Z}_2^n \to \mathbb{Z}_2$ известно [2, с. 78] псевдобулево представление в виде суммы

$$(-1)^{g(x)} = \sum_{a \in \mathbb{Z}_2^n} C(a, g)(-1)^{\langle a,x \rangle}, \quad \langle a, x \rangle = a_1 x_1 \oplus \ldots \oplus a_n x_n,$$

где $C(a, g) = 2^{-n} \sum\limits_{x \in \mathbb{Z}_2^n} (-1)^{\langle a,x \rangle + g(x)}$ — спектральный коэффициент функции g (нормированный коэффициент Уолша — Адамара).

Вектор $C(g) = \big(C(a, g) : a \in \mathbb{Z}_2^n\big)$ размерности 2^n называется *спектром булевой функции* g. Например, спектр функции-константы 0 равен $e_1 = (1, 0, \ldots, 0)$, где левая координата соответствует нулевому вектору. Здесь и далее через $e_i = (\underbrace{0, \ldots, 0}_{i-1}, 1, 0, \ldots, 0)$ обозначаем векторы стандартного базиса длины, определяемой контекстом.

Для двоичного вектора $x \in \mathbb{Z}_2^n$ через

$$w(x) = (w_a(x) : a \in \mathbb{Z}_2^n), \quad w_a(x) = (-1)^{\langle a,x \rangle},$$

обозначим соответствующий ему расширенный действительнозначный вектор, состоящий из псевдобулевых образов линейных комбинаций компонент x. Это даёт следующую краткую запись псевдобулева представления булевой функции:

$$(-1)^{g(x)} = w(x)C(g)^{\downarrow}, \quad x \in \mathbb{Z}_2^n. \tag{4}$$

Здесь и далее через $a^{\downarrow} = (a)^{\mathrm{T}}$ обозначаем вектор-столбцы.

Теперь перейдём к произвольной двоичной вектор-функции (булевому отображению) $g = (g_1, \ldots, g_m) : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$. Для неё представление (4) принимает вид

$$\text{если } y = g(x), \text{ то } w(y) = w(x)\Psi(g), \tag{5}$$

где $\Psi(g) = \|C(a, \langle b, g(x) \rangle)\|_{a \in \mathbb{Z}_2^n, b \in \mathbb{Z}_2^m} = \Big(e_1^{\downarrow}, C(g_1)^{\downarrow}, \ldots, C(g_1 \oplus \ldots \oplus g_m)^{\downarrow}\Big)$ — матрица размера $2^n \times 2^m$. Такие матрицы возникают во многих криптографических приложениях [3; 4, гл. 7; 5]. Тогда, как правило, $m = n$ и функции g являются биективными S-блоками.

При $m = n$ критерием биективности функции g является сбалансированность всех ненулевых линейных комбинаций её компонент, что эквивалентно равенству $\Psi(g)_0 = e_1$, а также ортогональности матрицы $\Psi(g)$ [3, с. 279; 5, теорема 3]. Заметим, что ранее А. С. Амбросимов доказал более общий критерий того, что вектор-функция над полем Галуа сохраняет равномерное распределение [6, теорема 3].

Для функции усложнения f схемы (1), аргумент которой состоит из двух частей, получим другое представление, которое даст возможность усреднить матрицы по случайной части k. Далее обозначим через $\|$ операцию конкатенации векторов.

Лемма 1. Если $y = f(x, k)$, то $w(y) = w(x)\Psi(f, w(k))$, где $\Psi(f, w)$ — матрица размера $2^m \times 2^m$ с элементами

$$\Psi(f, w)_{a,b} = \sum_{c \in \mathbb{Z}_2^n} C\left(a \| c, \langle b, f(x, k) \rangle\right) w_c, \quad w \in \mathbb{R}^{2^n}. \tag{6}$$

Доказательство. Обозначая $C(u,b) = C\left(u, \langle b, f(x,k)\rangle\right)$ для краткости, имеем представление

$$w_b(y) = \sum_{u \in \mathbb{Z}_2^{m+n}} C(u,b) w_u(x\|k).$$

Полагая $u = a\|c$, с учётом равенства $w_u(x\|k) = w_a(x)w_c(k)$ получаем

$$w_b(y) = \sum_{a \in \mathbb{Z}_2^m} w_a(x) \left(\sum_{c \in \mathbb{Z}_2^n} C(a\|c, b) w_c(k) \right) = w(x)\Psi(f, w(k))_b^{\downarrow},$$

что и требовалось доказать. ■

Из леммы 1 следует, что в схеме (1)

$$w(y) = w(x)\,\Psi(f, w(k(1)))\ldots\Psi(f, w(k(R))). \tag{7}$$

Поэтому $\Psi(f, w(k(r)))$ является матрицей связи входа и выхода r-го раунда.

1.2. Спектр распределения выходного случайного вектора

Преобладанием нуля в распределении двоичной случайной величины η называется число

$$\mathsf{E}(-1)^{\eta} = \mathsf{P}\{\eta = 0\} - \mathsf{P}\{\eta = 1\} = 2\,\mathsf{P}\{\eta = 0\} - 1 \in [-1, 1].$$

Спектром распределения двоичного случайного вектора ξ называется

$$\phi(\xi) = \mathsf{E}w(\xi)$$

— вектор, состоящий из преобладаний в распределениях всевозможных линейных комбинаций компонент вектора ξ.

Найдём формулу связи между спектрами входа и выхода одной итерации, а затем — формулу связи спектров входа и выхода всей схемы.

Теорема 1. Пусть в схеме (1) выполнено условие (2) независимости входа и ключевых векторов. Тогда

$$\phi\big(y(t)\big) = \phi\big(y(t-1)\big)\,\Psi\big(f, \phi(k(t))\big), \quad 1 \leqslant t \leqslant R,$$
$$\phi\big(y\big) = \phi(x)\,\Psi\big(f, \phi(k(1))\big)\ldots\Psi\big(f, \phi(k(R))\big).$$

Доказательство. Согласно лемме 1, для каждого $1 \leqslant t \leqslant R$

$$w(y(t)) = w(y(t-1))\Psi(f, w(k(t))). \tag{8}$$

Легко доказать, что если случайные матрицы $B_1, \ldots, B_l$ независимы (рассматриваем их как случайные векторы), то $\mathsf{E}(B_1 \ldots B_l) = \mathsf{E}B_1 \ldots \mathsf{E}B_l$. Как и ранее, под случайными вектором и матрицей мы понимаем наборы случайных величин, заданных на одном вероятностном пространстве.

Случайный вектор $y(t-1)$ не зависит от случайной матрицы $\Psi(f, w(k(t)))$, поскольку они являются соответственно функциями от независимых наборов случайных векторов $x, k(1), \ldots, k(t-1)$ и $\{k(t)\}$. Поэтому первая формула получается путём взятия математического ожидания от обеих частей (8) с учётом того, что $\mathsf{E}\Psi(f, w) = \Psi(f, \mathsf{E}w)$ для любого случайного действительнозначного вектора w.

Вторая формула аналогично вытекает из равенства (7). ■

Таким образом, матрица $\Psi(f, \phi(k(r)))$, полученная интегрированием (взятием математического ожидания) случайной матрицы $\Psi(f, w(k(r)))$, является *матрицей связи спектров* входа и выхода на r-м раунде.

Отметим, что спектр $\phi = \phi(\xi)$ распределения является набором всех значений характеристической функции [6, 7] случайного двоичного вектора $\xi = (\xi_1, \ldots, \xi_m)$ и поэтому полностью определяет распределение ξ [7, с. 102]. В более простом виде для случая группы вычетов $\mathbb{Z}_k$ формула обращения приведена в [8, с. 25]. Через спектр выражается, в частности, ковариационная матрица расширенного случайного вектора $w(\xi)$:

$$\Sigma\big(w(\xi)\big) = \|\phi_{a\oplus b} - \phi_a\phi_b\|_{a,b\in\mathbb{Z}_2^m}. \tag{9}$$

Эта формула легко следует из равенства $w_a(\xi)w_b(\xi) = w_{a\oplus b}(\xi)$.

1.3. Матрицы связи в случае покоординатного наложения раундовых ключей

Рассмотрим распространённую (в частности, используемую в PRESENT) схему аддитивного наложения раундовых ключей. Здесь $n = m$ и ключевой вектор накладывается посредством векторного сложения, то есть

$$f(x, k) = g(x \oplus k), \quad g : \mathbb{Z}_2^m \to \mathbb{Z}_2^m. \tag{10}$$

В этом случае выражение (6) для матрицы $\Psi(f, w)$ упрощается.

Теорема 2. Если функция f имеет вид (10), то столбцы матрицы связи равны

$$\Psi(f, w)_b^{\downarrow} = C(\langle b, g(x)\rangle)^{\downarrow} * w^{\downarrow}, \quad b \in \mathbb{Z}_2^m, \tag{11}$$

где $*$ — операция покоординатного умножения векторов.

Доказательство. Зафиксируем вектор b и, делая замену $y = x \oplus k$ в выражении для спектральных коэффициентов, имеем

$$C(a\|c, \langle b, f\rangle) = 2^{-2m} \sum_{x\in\mathbb{Z}_2^m, k\in\mathbb{Z}_2^m} (-1)^{\langle a,x\rangle+\langle c,k\rangle+\langle b,g(x\oplus k)\rangle} =$$

$$= 2^{-m} \sum_{x\in\mathbb{Z}_2^m} (-1)^{\langle a,x\rangle} \cdot 2^{-m} \sum_{y\in\mathbb{Z}_2^m} (-1)^{\langle c,x\oplus y\rangle+\langle b,g(y)\rangle} =$$

$$= 2^{-m} \sum_{x\in\mathbb{Z}_2^m} (-1)^{\langle a\oplus c,x\rangle} C(c, \langle b, g\rangle) = \begin{cases} 0, & a \neq c, \\ C(c, \langle b, g\rangle), & a = c. \end{cases}$$

Таким образом, из 2^{2m} коэффициентов $C(a\|c, \langle b, f(x, k)\rangle)$ ненулевыми могут быть лишь 2^m коэффициентов, у которых $a = c$. Тогда из леммы 1 получаем, что $\Psi(f, w)_{a,b} = C(a, \langle b, g\rangle)w_a$. ■

2. Критерий проверки гипотез

2.1. Спектральная формулировка гипотез

Справедлив спектральный критерий равномерности распределения случайного вектора [7, с. 102] (см. также более простую форму [8, с. 26]), который для двоичного вектора принимает вид

$$\xi \sim U(\mathbb{Z}_2^m) \iff \phi_a(\xi) = \mathbb{I}\{a = 0\}, \ a \in \mathbb{Z}_2^m, \tag{12}$$

где $\mathbb{I}\{A\}$ — индикатор выполнения условия A. Поэтому гипотеза H_1 эквивалентна тому, что $\phi(\xi) = e_1$. При этом

$$\Sigma\big(w(\xi)\big) = \operatorname{diag}(0, 1, \ldots, 1), \tag{13}$$

так как, согласно (9) и (12), $\Sigma_{a,b} = \mathbb{I}\{a = b\} - \mathbb{I}\{a = 0\}\mathbb{I}\{b = 0\}$. Левый верхний элемент ковариационной матрицы равен 0, поскольку $w_0(\xi) \equiv 1$.

Далее считаем, что распределение выхода схемы неравномерно, т. е.

$$\phi(y) \neq e_1, \tag{14}$$

что даёт принципиальную возможность построения атаки различения. Получим условие, необходимое для (14).

Лемма 2. Если $k \sim U(\mathbb{Z}_2^n)$, то f биективна тогда и только тогда, когда $\Psi(f, \phi(k))_0 = e_1$.

Доказательство. Из леммы 1 с учётом критерия (12) и вышеупомянутого критерия [3] биективности функции получаем, что элементы верхней строки матрицы $\Psi = \Psi(f, w(k))$ равны

$$\Psi_{0,b} = \sum_{c \in \mathbb{Z}_2^n} C\left(0 \| c, \langle b, f(x,k)\rangle\right) \mathbb{I}\{c = 0\} = C\left(0, \langle b, f(x,k)\rangle\right) = \mathbb{I}\{b = 0\},$$

что и требовалось доказать. ■

Из теоремы 1 и леммы 2 следует, что в случае биективной функции f (что часто выполнено для функций усложнения блочных шифрсистем) для (14) необходимо, чтобы

$$\phi(x) \neq e_1 \text{ или } \phi(k(t)) \neq e_1 \text{ для некоторого } 1 \leqslant t \leqslant R, \tag{15}$$

т. е. чтобы вход или хотя бы один ключевой вектор были распределены неравномерно.

2.2. Построение и расчёт критерия

Пусть далее E — единичная матрица, размер которой определяется контекстом, $\Phi(x)$ — функция распределения стандартного нормального закона $\mathcal{N}(0,1)$, κ_γ — квантиль уровня γ распределения $\mathcal{N}(0,1)$, т. е. $\Phi(\kappa_\gamma) = \gamma$. Нам потребуется следующее вспомогательное утверждение о многомерных нормальных распределениях.

Лемма 3. Пусть $\alpha \in (0,1)$, $\mu \neq 0$, $\nu = \mu/|\mu|$ — вектор евклидовой нормы 1, сонаправленный с μ. Тогда

$$\mathsf{P}\{\eta\,\nu^{\downarrow} \leqslant \kappa_{1-\alpha}\} = \begin{cases} 1-\alpha \text{ при } \eta \sim \mathcal{N}(0, E), \\ \Phi\left(\dfrac{\kappa_{1-\alpha} - |\mu|}{\sigma}\right) \text{ при } \eta \sim \mathcal{N}(\mu, \Sigma) \end{cases}$$

для любой ковариационной матрицы Σ, вырожденной или невырожденной, если $\sigma^2 = \nu\,\Sigma\nu^{\downarrow} > 0$.

Доказательство. Известно, что если η имеет нормальное распределение, вырожденное или невырожденное, то любая линейная комбинация его компонент $\zeta = \eta\,\nu^{\downarrow}$ имеет нормальное распределение со средним $(\mathsf{E}\eta)\,\nu^{\downarrow}$ и дисперсией $\nu\Sigma\nu^{\downarrow}$. Тогда при $\eta \sim \mathcal{N}(0, E)$ имеем $\mathsf{E}\zeta = 0$, $\mathsf{D}\zeta = \nu\nu^{\downarrow} = |\nu|^2 = 1$, и искомая вероятность равна $\Phi(\kappa_{1-\alpha}) = 1 - \alpha$. При $\eta \sim \mathcal{N}(\mu, \Sigma)$ имеем $\mathsf{E}\zeta = \mu\nu^{\downarrow} = |\mu|$, $\mathsf{D}\zeta = \nu\,\Sigma\nu^{\downarrow} = \sigma^2$, и вероятность равна $\mathsf{P}\left\{(\zeta - |\mu|)/\sigma \leqslant (\kappa_{1-\alpha} - |\mu|)/\sigma\right\} = \Phi\left((\kappa_{1-\alpha} - |\mu|)/\sigma\right)$. ■

Для двоичного вектора $x \in \mathbb{Z}_2^m$ через $\tilde{w}(x) = (w_a(x) : 0 \neq a \in \mathbb{Z}_2^m)$ обозначим действительнозначный вектор размерности $2^m - 1$, полученный удалением из $w(x)$ крайней левой компоненты, тождественно равной 1, и рассмотрим статистику

$$S(N) = \tilde{w}\left(\xi^{(1)}\right) + \ldots + \tilde{w}\left(\xi^{(N)}\right)$$

— сумму независимых одинаково распределённых случайных векторов согласно условию (3).

Согласно центральной предельной теореме [9, с. 435], при $N \to \infty$ распределение нормированной статистики сходится к нормальному:

$$\frac{1}{\sqrt{N}}(S(N) - N\mathsf{E}\tilde{w}(\xi)) \xrightarrow{D} \mathcal{N}(0, \Sigma(\tilde{w}(\xi))).$$

Отсюда с учётом (12) и (13) следует, что при гипотезе H_1 предельное распределение будет стандартным нормальным: $\dfrac{S(N)}{\sqrt{N}} \xrightarrow{D} \mathcal{N}(0, E)$.

Итак, получаем критерий

$$S(N)\,\nu^{\downarrow} > \sqrt{N}\kappa_{1-\alpha} \Longrightarrow H_2, \tag{16}$$

где $\nu = \tilde{\phi}(y)/|\tilde{\phi}(y)|$; $\tilde{\phi}(y)$ — вектор, полученный из $\phi(y)$ отбрасыванием левой координаты. Его критической областью является полупространство, отделённое от начала координат гиперплоскостью, перпендикулярной вектору, направленному от 0 к $\tilde{\phi}(y)$.

Из леммы 3 и теоремы непрерывности 2 [9, с. 32] следует, что критерий имеет асимптотический размер α, т. е. $\alpha_1(N) \to \alpha$ при $N \to \infty$ для любого фиксированного $\alpha \in (0, 1)$.

Оценим вероятность ошибки второго рода. При гипотезе H_2 и больших N распределение $\dfrac{S(N)}{\sqrt{N}}$ близко к $\mathcal{N}(\sqrt{N}\tilde{\phi}(y), \tilde{\Sigma})$, где $\tilde{\Sigma} = \Sigma(\tilde{\phi}(y)))$ может быть получена из матрицы (9), вычисленной при $\xi = y$, путём отбрасывания верхней строки и левого столбца. Тогда по лемме 3

$$\alpha_2(N) \approx \Phi\left(\frac{\kappa_{1-\alpha} - \sqrt{N}|\tilde{\phi}(y)|}{\sigma}\right), \text{ где } \sigma^2 = \nu\,\tilde{\Sigma}\nu^{\downarrow}.$$

Следовательно, значение $\alpha_2(N)$ будет близко к заданному значению $\beta \in (0, 1)$ при

$$N = N^*(\alpha, \beta) = \frac{(\kappa_{1-\alpha} + \kappa_{1-\beta}\sigma)^2}{|\tilde{\phi}(y)|^2}. \tag{17}$$

3. Атака различения на SP-сеть с независимыми раундовыми ключами

Критерий для проверки гипотезы H_1 против H_2 в криптографической литературе называется *атакой различения* на заданную схему. Для построения критерия требуется знание распределения y выхода схемы. Рассмотрим возможные способы его вычисления. Если ключи $k(t)$ извлекаются равновероятно из некоторых ключевых множеств $K(t) \subset \mathbb{Z}_2^n$, а x из $X \subset \mathbb{Z}_2^m$, то поиск распределения выхода путём тотального вычисления всех значений $y = y(x, k(1), \ldots, k(R))$ имеет сложность, пропорциональную $|X| \cdot |K(1)| \cdot \ldots \cdot |K(R)|$. Если все ключевые множества имеют мощность K, то с ростом R эта сложность растет как K^R, т. е. экспоненциально. Другой путь поиска распределения даёт матричная формула теоремы 1: здесь временная сложность равна сложности вычисления произведения R матриц, что при росте R и фиксированном m оценивается величиной, линейно зависящей от R. Справедливости ради заметим, что при этом способе сравнительно большое значение имеет емкостная сложность хранения матриц Ψ, пропорциональная величине 2^{2m}.

Заметим также, что существует ещё путь статистического оценивания распределения y при случайном выборе $x, k(1), \ldots, k(R)$, но его исследование выходит за рамки данной работы.

Перейдём к выбору схемы шифрования, а также распределений входного блока и раундовых ключей. Схемы шифрования были выбраны из семейства SmallPresent[m] [1] масштабируемых моделей шифрсистемы PRESENT, у которых длина блока m, измеряемая в битах, кратна 4. Так как шифрсистема является SP-сетью с покоординатным наложением раундовых ключей, то $m = n$ и матрица связи вычисляется по формуле (11). Из-за большого размера $2^m \times 2^m$ матрицы Ψ мы были вынуждены ограничиться сравнительно небольшими значениями $m \leqslant 12$. Оригинальный алгоритм получения раундовых ключей заменён на описываемую ниже схему (19) их случайной генерации, что назовём *неавтономной моделью*. Поскольку должно быть обеспечено условие (3) независимости наблюдаемых блоков, наборы раундовых ключей будут выбираться независимо для каждого входного блока, что соответствует ситуации *«много одноблочных сообщений»*.

Ограничимся случаем, когда все раундовые ключи распределены одинаково: $k(t) \sim k$, и тогда при условии (2)

$$\phi(y) = \phi(x)\Psi(f, \phi(k))^R. \tag{18}$$

Согласно (15), распределение x или k должно быть неравномерным. Будем использовать модель, в которой все биты этих векторов выбираются независимо с преобладанием $d \neq 0$, т. е. каждый бит имеет распределение Бернулли $\mathrm{Be}\left(\dfrac{1-d}{2}\right)$, и обозначать это так:

$$x \sim k \sim \mathrm{Be}^m\left(\frac{1-d}{2}\right). \tag{19}$$

Заметим, что тогда

$$\phi(x) = \phi(k) = (d^{\|a\|} : a \in \mathbb{Z}_2^m) = (1, d, \ldots, d^m).$$

Далее описаны эксперименты двух типов: 1) построение критериев (16) и оценки их характеристик; 2) сравнение их с критерием «стопка книг», далее называемым «СК-тест» для краткости.

3.1. Эксперименты по построению и применению критерия

Здесь целью экспериментов является построение критерия, проверка соответствия реально наблюдаемых ошибок критерия (16) и заданных значений α, β. Для этого проводилось $M = 50$ серий получения выборок при каждой гипотезе. Опишем методику проведения экспериментов.

1. Для заданных распределений x и k и функции f находим спектры $\phi(x), \phi(k)$, матрицу $\Psi(f, \phi(k))$, а затем спектр $\phi(y)$ по формуле (18).

2. Вычисляем $\tilde{\phi}(y)$, ν, $\tilde{\Sigma}$ и $N = N^*(\alpha, \beta)$ для заданных значений α, β согласно (17).

3. Генерируем независимо M выборок $\xi^{(t)}$, $1 \leqslant t \leqslant M$, объёма N по случайной равновероятной схеме, применяем к каждой выборке критерий. Получаем значение $\hat{\alpha} = M_2/M$, где M_2 — количество решений в пользу H_2.

4. Генерируем независимо M серий по N независимых наборов $(x, k(1), \ldots, k(R))$ в соответствии с заданными распределениями, применяем к каждому набору схему шифрования, получаем выборку $\xi^{(t)}$ из N выходных векторов схемы. Применяя к каждой выборке критерий, находим значение $\hat{\beta} = M_1/M$, где M_1 — количество решений в пользу H_1.

Здесь взято число раундов $R = 10$ и значения $\alpha = \beta = 0{,}2$ выбраны достаточно большими для того, чтобы при небольшом числе $M = 50$ серий математическое ожидание значения $\hat{\alpha}$ было не очень мало. Графики зависимости $N^*(\alpha, \beta)$ от значений преобладания d представлены на рис. 1.

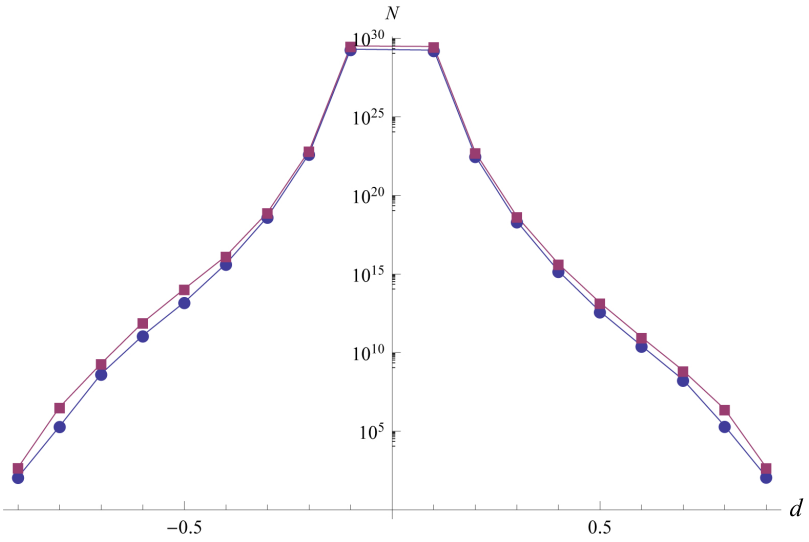

Рис. 1. Зависимость $N^*(\alpha, \beta)$ от d для моделей SmallPresent$[m]$, $m = 8, 12$

Заметим, что на рис. 1 вычисленные значения $N^*(\alpha, \beta)$ монотонно зависят от $|\tilde{\phi}(y)|$. Это, вообще говоря, не следует из (17), поскольку в числителе этой формулы σ также зависит от $\tilde{\phi}(y)$.

Численные результаты экспериментов для некоторых значений преобладания d представлены в табл. 1. Реальные вероятности шестнадцати полученных ошибок критерия (16) лежат в пределах от 0,06 до 0,3, что согласуется с теорией.

Таблица 1

Результаты экспериментов с неавтономными моделями SmallPresent$[m]$ при $R = 10$, $M = 50$, $\alpha = \beta = 0{,}2$, $x \sim k \sim \mathrm{Be}^m\left(\dfrac{1-d}{2}\right)$ в ситуации одноблочных сообщений

Параметры	SmallPresent[8]				SmallPresent[12]			
d	-0,9	-0,8	0,8	0,9	-0,9	-0,8	0,8	0,9
$\lvert\tilde{\phi}(y)\rvert$	0,21	$3{,}6 \cdot 10^{-3}$	$3{,}63 \cdot 10^{-3}$	0,20	0,11	$9{,}08 \cdot 10^{-4}$	$1{,}0 \cdot 10^{-3}$	0,11
σ^2	3,01	1,69	0,99	3,02	3,73	1,0	1,0	3,66
$N_1(\alpha, \beta, d)$	121	$2{,}7 \cdot 10^5$	$2{,}14 \cdot 10^5$	127	501	$3{,}4 \cdot 10^6$	$2{,}5 \cdot 10^6$	492
$\widehat{\alpha}$	0,22	0,06	0,22	0,24	0,24	0,30	0,10	0,08
$\widehat{\beta}$	0,20	0,20	0,16	0,12	0,16	0,06	0,10	0,18

Так как при уменьшении $|d|$ распределение $\mathrm{Be}^m\left(\dfrac{1-d}{2}\right)$ приближается к равномерному, т. е. гипотезы сближаются, то значение $|\tilde{\phi}(y)|$ уменьшается, а объём материала $N^*(\alpha, \beta, d)$ увеличивается. Поэтому для $|d| \leqslant 0{,}7$ статистические эксперименты не проводились.

3.2. Эксперименты для сравнения критерия и СК-теста

СК-тест и предлагаемая его модификация

На основе адаптивной структуры «стопка книг», которая предложена Б. Я. Рябко в 1980 г., позже был построен СК-тест. Он является одним из мощных универсальных тестов для проверки гипотезы о равновероятности исходов в статистических моделях с S исходами, где S значительно больше объёма выборки. С 2004 г. он применялся в ряде работ [10 – 13] для оценки качества псевдослучайных последовательностей, вырабатываемых поточными шифрсистемами, а также блочными шифрсистемами в режиме CTR — так называется режим работы, в котором входной блок с номером $t = 0, 1, \ldots$ является m-битовым двоичным представлением числа t, т. е. это режим «счётчика».

Далее ограничимся часто применяемой версией СК-теста, в которой множество X исходов, $|X| = S$, разбивается на два множества, и первое из них (верхняя часть стопки) имеет мощность $Q \ll S$. В наших обозначениях эта версия описывается так: фиксируется A_1 — произвольный список, содержащий Q различных элементов X. Далее для наблюдаемой случайной последовательности блоков $\xi^{(1)}, \ldots, \xi^{(N)}$ рекуррентно строится последовательность $\{A_t\}$ случайных списков мощности Q, где A_{t+1} определяется по A_t и $\xi^{(t)}$ следующим образом. Элемент $\xi^{(t)}$ становится первым элементом A_{t+1} и к нему присоединяется список A'_t мощности $Q-1$, где A'_t получен из A_t удалением $\xi^{(t)}$ при $\xi^{(t)} \in A_t$ либо удалением последнего элемента A_t при $\xi^{(t)} \notin A_t$. Рассматривается статистика

$$\nu = \sum_{1 \leqslant t \leqslant N} \mathbb{I}\{\xi^{(t)} \in A_t\}.$$

Лемма 4. При гипотезе H_1 о независимости и равновероятности блоков события $\{\xi^{(t)} \in A_t\}$ независимы и статистика имеет биномиальное распределение $\nu \sim \mathrm{Bin}(N, q)$, $q = Q/S$.

Доказательство. Заметим, что при фиксированном значении A_1 фиксация значений $\xi^{(1)} = a_1, \ldots, \xi^{(t-1)} = a_{t-1}$ однозначно определяет значение случайного списка A_t, $t \geqslant 1$, которое обозначим через

$$B_t = B_t(A_1, a_1, \ldots, a_{t-1}).$$

Тогда для любых $k \geqslant 1$ фиксированных номеров $1 \leqslant t_1 < \ldots < t_k = T$, обозначая $l = T - k$, $\{s_1, \ldots, s_l\} = \{1, \ldots, T\} \setminus \{t_1, \ldots, t_k\}$, имеем

$$\mathsf{P}\left\{\xi^{(t_1)} \in A_{t_1}, \ldots, \xi^{(t_k)} \in A_{t_k}\right\} =$$

$$= \sum_{a_{s_1}, \ldots, a_{s_l} \in X} \mathsf{P}\left\{\xi^{(t_1)} \in A_{t_1}, \ldots, \xi^{(t_k)} \in A_{t_k}, \xi^{(s_1)} = a_{s_1}, \ldots, \xi^{(s_l)} = a_{s_l}\right\} =$$

$$= \sum_{a_{s_1}, \ldots, a_{s_l} \in X} \sum_{a_{t_1} \in B_{t_1}} \cdots \sum_{a_{t_k} \in B_{t_k}} \mathsf{P}\left\{\xi^{(1)} = a_1, \ldots, \xi^{(T)} = a_T\right\} = S^l Q^k \frac{1}{S^T} = \left(\frac{Q}{S}\right)^T = q^k,$$

поскольку все вероятности в последней сумме равны $1/S^T$ и каждое множество B_{t_i} содержит ровно Q элементов.

При $k = 1$ получаем $\mathsf{P}\left\{\xi^{(t)} \in A_t\right\} = q$ для всех $t \geqslant 1$, и поэтому

$$\mathsf{P}\left\{\xi^{(t_1)} \in A_{t_1}, \ldots, \xi^{(t_k)} \in A_{t_k}\right\} = \mathsf{P}\left\{\xi^{(t_1)} \in A_{t_1}\right\} \ldots \mathsf{P}\left\{\xi^{(t_k)} \in A_{t_k}\right\}.$$

Лемма 4 доказана. ■

В упомянутых работах рассматривается статистика типа «хи-квадрат»

$$x^2 = \frac{(\nu - Nq)^2}{Nq} + \frac{((N-\nu) - N(1-q))^2}{N(1-q)} = \frac{(\nu - Nq)^2}{Nq(1-q)} = \tilde{\nu}^2. \tag{20}$$

Она является квадратом случайной величины $\tilde{\nu} = \dfrac{\nu - Nq}{\sqrt{Nq(1-q)}}$, распределение которой с учётом леммы 4 сходится к $\mathcal{N}(0,1)$ при $N \to \infty$ и фиксированном q. Следовательно, $x^2 \xrightarrow{D} \chi_1^2$ при гипотезе H_1, что неоднократно использовалось, но строгого доказательства этого факта нам найти не удалось.

В [14] изучается, а в [12, 13] применяется следующий критерий согласия с H_1: если $x^2 \geqslant \kappa(1-\alpha, \chi_1^2)$, где κ — квантиль распределения χ_1^2, то H_1 отклоняется. Он имеет асимптотический размер α и эквивалентен двустороннему критерию

$$\text{если } |\tilde{\nu}| \geqslant \kappa_{1-\alpha/2}, \text{ то } H_1 \text{ отклоняется}, \tag{21}$$

где κ_γ — квантиль распределения $\mathcal{N}(0,1)$, как и раньше.

Как отмечается в [10, с. 74], при альтернативе о неравновероятности исходов в выборке чаще появляются более вероятные исходы, и они проводят в верхней части стопки значительно больше времени, чем остальные. Но это всегда ведет к смещению распределения ν вправо от Nq, и, по нашему мнению, при независимых наблюдениях более адекватен следующий односторонний критерий:

$$\text{если } \nu \geqslant Nq + \kappa_{1-\alpha}\sqrt{Nq(1-q)}, \text{ то } H_1 \text{ отклоняется} \tag{22}$$

асимптотического размера α. Этот модифицированный СК-тест для краткости далее называем *МСК-тестом*.

Заметим, что двусторонний критерий (21) также выявляет смещение распределения ν влево от Nq. Такое смещение возникает, например, когда наблюдения зависимы и появление элемента в выборке уменьшает эмпирическую вероятность его появления. В частности, это соответствует альтернативе, при которой выбор элементов происходит случайно без возвращения.

При гипотезе типа H_2 строгий расчёт тестов является сложной задачей, поскольку в общем случае распределение статистик будет зависеть от конкретного ключа (например, в экспериментах [11, табл. 1] эмпирическая ошибка 2-го рода адаптивного теста χ^2 при его применении к выходным последовательностям длины $N = 2^{20}$ блоков трехраундового RC5 ($m = 64$) изменялась от 0,95 до 0,01 в зависимости от ключа шифрования; эксперименты проводились для 10 случайных ключей). Для универсальных тестов, вероятно, задача ещё более усложняется, поскольку они не «подстроены» под конкретную шифрсистему; авторы не встречались с примерами её строгого решения. Это главная причина отсутствия теоретического сравнения вероятностей ошибок 2-го рода нашего критерия с другими тестами, и далее проводится его экспериментальное сравнение с СК- и МСК-тестами.

Здесь можно добавить, что в [14] изучается распределение статистики x^2 при альтернативе $H^{\gamma,\delta}$, $\gamma, \delta \in (0,1)$, заключающейся в том, что в схеме с S исходами некоторые $S\gamma$ исходов имеют вероятность $(1+\delta)/S$, некоторые $S\gamma$ исходов имеют вероятность $(1-\delta)/S$, а оставшиеся $S(1-2\gamma)$ исходов имеют вероятность $1/S$. Получена следующая асимптотическая оценка для объёма выборки: для любых $\alpha, \beta \in (0,1)$ существует

такое $C > 0$, что при $S \to \infty$ вероятности ошибок СК-теста (21) с $|A_1| = [\sqrt{S}]$ асимптотически не превосходят α и β соответственно, если

$$N = C[\sqrt{S}]. \tag{23}$$

Признавая силу и универсальность СК-теста, считаем необходимым сделать следующие замечания по поводу методики его применения [13].

1. Если главная цель [13] — изучение проблемы создания быстрого генератора псевдослучайных последовательностей на базе блочных шифрсистем («сокращение числа раундов увеличит производительность шифров и позволит генерировать псевдослучайные числа быстрее» [13, с. 66]), то представляется не вполне обоснованным: а) выбор слабой CTR-последовательности в качестве входа (можно рассмотреть, например, более сильный и простой режим, при котором входным блоком шифрсистемы является предыдущий выходной блок); б) ограничение только первым выходным 32-битным словом (из 2–4 возможных в зависимости от $64 \leqslant m \leqslant 128$).

2. Как отмечалось выше со ссылкой на [10, с. 74], неравновероятность исходов в выборке смещает распределение ν вправо от Nq (применяемая версия СК-теста сводится к этой статистике согласно равенствам (20)). Но режим CTR в силу биективности блочного преобразования эквивалентен выбору без возвращения, что должно было привести к значительному (при любом числе раундов!) смещению распределения ν влево. Редуцирование выходного блока до одного слова размывает этот эффект (это, возможно, является объяснением обстоятельства $1, б$), и неясно, на что сильнее в итоге реагирует СК-тест, т. е. куда сместится распределение ν. Ответ на этот вопрос могли бы дать средние экспериментальные значения $\tilde{\nu}$. Если они большие (по абсолютной величине) отрицательные, то построенный в [13] критерий реагирует на выбор блоков без возвращения, а не на их неравновероятность.

Эксперименты с моделью SmallPresent[12]

Проведём сравнительный экспериментальный анализ нашего критерия и СК-теста (21), МСК-теста (22) при выборе значения их параметра

$$Q = 2^{m/2} = 2^6 = 64$$

согласно условию (23), принятому также в [13]. Число раундов R растёт от 3 до 10, количество серий $M = 10$, расчётные вероятности ошибок $\alpha = 0{,}05$, $\beta = 0{,}01$, набор из R раундовых ключей случайно выбирается для каждого N_2-блочного сообщения. Как и раньше, каждый из R ключей выбирается по схеме $k \sim \mathrm{Be}^{12}\left(\dfrac{1-d}{2}\right)$, $d = 0{,}8$. В частности, при $N_2 = 1$ получаем ранее исследованную ситуацию одноблочных сообщений.

Количество сообщений $N_1 = [N^*(R, \alpha, \beta, d)/N_2]$ взято таким, чтобы общий их объём, измеряемый в блоках, был близок к расчётному объёму выборки (17) нашего критерия (табл. 2).

Входные блоки выбираются независимо и равновероятно из множества слов с восемью нулевыми старшими битами:

$$x(t) \sim U(V), \quad V = \left\{x \in \mathbb{Z}_2^{12} : \; x_1 = \ldots = x_8 = 0\right\}, \tag{24}$$

что близко к режиму CTR, но, в отличие от него, $x(1), \ldots, x(N)$ независимы и неизвестны. Этот режим выбора можно назвать *известным неравномерным распределением неизвестных входных блоков*. Значение параметра 8 в (24) выбрано таким, чтобы

Таблица 2

Объём материала, достаточный для корректной работы спектрального критерия при различном значении количества раундов R шифрсистемы SmallPresent[12]

R	3	4	5	6	7	8	9	10
$N^*(R)$	18	65	363	$2{,}7 \cdot 10^3$	$1{,}9 \cdot 10^4$	$1{,}2 \cdot 10^5$	$8{,}8 \cdot 10^5$	$7{,}3 \cdot 10^6$

максимальная доля ненулевых битов в блоке, равная $\dfrac{12-8}{12} = \dfrac{1}{3}$, была близка к максимальной доле $\dfrac{24}{64} = \dfrac{3}{8}$ ненулевых битов в блоке в экспериментах [13].

Итак, в каждой серии выполняем следующие шаги:

1) Для фиксированного $R = 3, 4, \ldots$ выбираем из табл. 2 значение $N = N^*(R, \alpha, \beta, d) = N^*(R)$. Случайно равновероятно из V выбираем N_2 блоков открытого текста и формируем из них сообщения длины N_2. Генерируем таким образом $\lceil N/N_2 \rceil$ сообщений.
2) Для каждого сообщения, согласно указанному выше распределению, выбираем случайно набор из R раундовых ключей и шифруем на этом наборе все блоки сообщения. Объединяем вместе блоки всех сообщений в единую выборку.
3) Применяем к полученной выборке спектральный критерий, СК-тест и МСК-тест.

По результатам M серий вычисляем вектор эмпирических вероятностей ошибок $\beta = (\widehat{\beta}_1, \widehat{\beta}_2, \widehat{\beta}_3)$, которые равны отношению к M количества серий, в которых соответствующий тест неправильно принял решение, а также $\widetilde{\nu}_{\text{ср}}$ — эмпирическое среднее значение статистики $\tilde{\nu}$ по сериям. Эти значения представлены в табл. 3 — вектор $\beta \cdot M$ в верхней строке и $\widetilde{\nu}_{\text{ср}}$ в нижней для каждого N_2.

Таблица 3

Результаты экспериментов в модели «много коротких сообщений» для шифрсистемы SmallPresent[12]

N_2	R							
	3	4	5	6	7	8	9	10
1	0, 9, 9	0, 8, 8	1, 9, 8	0, 9, 9	1, 10, 9	1, 9, 9	1, 10, 10	1, 9, 9
	0,20	1,98	−0,28	−0,20	0,29	−0,30	−0,14	−0,20
2	1, 8, 8	1, 5, 5	1, 2, 0	1, 0, 0	1, 0, 0	1, 0, 0	2, 0, 0	1, 0, 0
	1,50	3,98	4,49	11,4	34,4	87,57	231,9	668,1
3	3, 2, 2	1, 2, 2	0, 0, 0	1, 0, 0	1, 0, 0	0, 0, 0	1, 0, 0	0, 0, 0
	3,45	5,08	10,25	25,13	67,10	172,32	455,77	1311,49
4	1, 4, 4	2, 0, 0	1, 0, 0	0, 0, 0	1, 0, 0	1, 0, 0	1, 0, 0	0, 0, 0
	2,69	5,88	14,73	37,74	98,48	252,65	669,64	1929,11
5	1, 2, 2	4, 0, 0	1, 0, 0	0, 0, 0	0, 0, 0	1, 0, 0	0, 0, 0	0, 0, 0
	5,16	7,18	18,9	48,27	129,12	330,7	874,07	2516,76
6	4, 2, 2	2, 0, 0	1, 0, 0	1, 0, 0	1, 0, 0	0, 0, 0	0, 0, 0	2, 0, 0
	4,78	9,08	21,26	59,86	159,16	406,80	1070,59	3085,88
7	1, 2, 2	2, 0, 0	2, 0, 0	0, 0, 0	1, 0, 0	1, 0, 0	0, 0, 0	1, 0, 0
	6,30	9,88	26,03	70,1	186,34	476,00	1258,59	3628,72
8	4, 0, 0	3, 0, 0	3, 0, 0	1, 0, 0	3, 0, 0	0, 0, 0	2, 0, 0	1, 0, 0
	7,63	11,29	27,81	78,40	213,51	546,40	1440,21	4148,2
9	3, 0, 0	2, 0, 0	3, 0, 0	2, 0, 0	1, 0, 0	0, 0, 0	0, 0, 0	0, 0, 0
	8,20	13,08	32,64	88,74	240,14	611,14	1613,08	4649,34

Из табл. 3 можно сделать следующие выводы:

1) При $N_2 = 1$ для всех R, а также при $N_2 = 2$ для небольшого объёма материала (случаи $R = 3, 4$) спектральный критерий работает явно лучше обоих тестов. В других случаях СК-тест и МСК-тест работают лучше нашего критерия, а распределение статистики $\widetilde{\nu}$ смещается вправо от нуля, и значение $\widetilde{\nu}_{\text{ср}}$ растёт при увеличении R. Для объяснения причин этого эффекта требуется дополнительное теоретическое исследование тестов.
2) Значение эмпирической вероятности ошибки спектрального критерия при достаточном объёме материала остаётся близким к расчётному при всех $N_2 \geqslant 2$, если число сообщений достаточно большое. Это условие примерно соответствует значениям в табл. 3 выше главной диагонали.

Заключение

В работе получена матричная формула для спектра распределения выходных блоков итеративной схемы в зависимости от распределения входных блоков и распределения независимых раундовых (итерационных) ключей. Емкостная сложность её применения оценивается величиной $\mathrm{O}(2^{m^2})$, где m бит — длина блока. Временная сложность оценивается величиной $\mathrm{O}(R\,2^{m^2})$, где R — число раундов, и может быть значительно меньше тотальной сложности вычисления распределения выходных блоков, в ряде случаев близкой к $\mathrm{O}(2^{m^2+mR})$.

Первой особенностью вероятностной модели является случайный выбор раундовых ключей, что позволяет исключить зависимость распределения выходных блоков, а также основанной на спектре распределения атаки различения от конкретного ключа шифрования. Второй особенностью является предположение о том, что зашифрование каждого входного блока производится на своём случайном наборе раундовых ключей. Вместе это даёт возможность рассчитать оценки вероятностей ошибок атаки и объём выборки без использования каких-либо эвристических предположений. Условия атаки — известные неравномерные распределения неизвестных входных блоков и раундовых ключей. Эксперименты на мини-моделях блочной шифрсистемы PRESENT с длиной блока 12 битов и числом раундов $R \leqslant 10$ показали, что согласие с теорией сохраняется при произвольном количестве N_2 блоков, шифруемых на одном наборе раундовых ключей (несмотря на то, что при этом нарушается условие (3) независимости наблюдаемых блоков), если количество сообщений также большое.

Построенная атака различения учитывает внутреннее строение шифрсистемы и распределение входных блоков, что представляется большим потенциальным преимуществом по сравнению с универсальными статистическими критериями. Произведено экспериментальное сравнение построенного критерия с тестом «стопка книг», а также с предложенной его модификацией. Оно показало, что: 1) модификация работала не хуже оригинального теста во всех экспериментах; 2) критерий работал лучше модификации при $N_2 = 1$, а также при $N_2 \geqslant 2$ на небольшом количестве сообщений.

Авторы выражают признательность рецензенту за ряд полезных замечаний, способствовавших улучшению статьи.

ЛИТЕРАТУРА

1. *Leander G.* Small Scale Variants of the Block Cipher PRESENT. Technical University of Denmark, 2010. `http://eprint.iacr.org/2010/143.pdf`.
2. *Логачев О. А., Сальников А. А., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.

3. *Daemen J., Govaerts R., and Vandewalle J.* Correlation matrices // FSE-1995. LNCS. 1995. V. 1008. P. 275–285.
4. *Daemen J. and Rijmen V.* The design of Rijndael: AES — the Advanced Encryption Standard. Springer, 2002. 227 p.
5. *Денисов О. В.* Статистическая оценка множества существенных аргументов двоичной вектор-функции с искаженными значениями // Матем. вопр. криптографии. 2014. Т. 5. Вып. 4. С. 41–61.
6. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями // Дискретная математика. 1994. Т. 6. Вып. 3. С. 50–60.
7. *Воробьев Н. Н.* Сложение независимых случайных величин на конечных абелевых группах // Матем. сборник. 1954. Т. 34(76). Вып. 1. С. 83–126.
8. *Денисов О. В.* Вероятностные свойства двоичных отображений. Учеб.-методич. пособие. М., 2008. 80 с.
9. *Боровков А. А.* Математическая статистика. М.: Наука, 1984. 472 с.
10. *Рябко Б. Я., Пестунов А. И.* «Стопка книг» как новый статистический тест для случайных чисел // Проблемы передачи информации. 2004. Т. 40. № 1. С. 73–78.
11. *Рябко Б. Я., Монарев В. А., Шокин Ю. И.* Новый тип атак на блоковые шифры // Проблемы передачи информации. 2005. Т. 41. № 4. С. 97–107.
12. *Лысяк А. С., Рябко Б. Я., Фионов А. Н.* Анализ эффективности градиентной статистической атаки на блоковые шифры RC6, MARS, CAST-128, IDEA, Blowfish в системах защиты информации // Вестник СибГУТИ. 2013. № 1. С. 85–109.
13. *Пестунов А. И.* Предварительная оценка минимального числа раундов легковесных шифров для обеспечения их удовлетворительных статистических свойств // Прикладная дискретная математика. Приложение. 2015. № 8. С. 66–68.
14. *Пестунов А. И.* Теоретическое исследование свойств статистического теста «стопка книг» // Вычислительные технологии. 2006. Т. 11. № 6. С. 96–103.

REFERENCES

1. *Leander G.* Small Scale Variants of the Block Cipher PRESENT. Technical University of Denmark, 2010. `http://eprint.iacr.org/2010/143.pdf`.
2. *Logachev O. A., Sal'nikov A. A., and Yashchenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2004. (in Russian)
3. *Daemen J., Govaerts R., and Vandewalle J.* Correlation matrices. FSE-1995, LNCS, 1995, vol. 1008, pp. 275–285.
4. *Daemen J. and Rijmen V.* The design of Rijndael: AES — the Advanced Encryption Standard. Springer, 2002. 227 p.
5. *Denisov O. V.* Statisticheskaya otsenka mnozhestva sushchestvennykh argumentov dvoichnoy vektor-funktsii s iskazhennymi znacheniyami [Statistical estimation of the significant arguments set of the binary vector-function with corrupted values]. Mat. Vopr. Kriptogr., 2014, vol. 5, iss. 4, pp. 41–61. (in Russian)
6. *Ambrosimov A. S.* Svoystva bent-funktsiy q-znachnoy logiki nad konechnymi polyami [Properties of bent functions of q-valued logic over finite fields]. Diskr. Mat., 1994, vol. 6, iss. 3, pp. 50–60. (in Russian)
7. *Vorob'ev N. N.* Slozhenie nezavisimykh sluchaynykh velichin na konechnykh abelevykh gruppakh [Addition of independent random variables on finite abelian groups]. Mat. Sb., 1954, vol. 34(76), no. 1, pp. 89–126. (in Russian)

8. *Denisov O. V.* Veroyatnostnye svoystva dvoichnykh otobrazheniy [Probabilistic Properties of Binary Maps]. Uchebno-metodicheskoe posobie. Moscow, 2008. (in Russian)
9. *Borovkov A. A.* Matematicheskaya statistika [Mathematical statistics]. Moscow, Nauka Publ., 1984. (in Russian)
10. *Ryabko B. Ya. and Pestunov A. I.* «Stopka knig» kak novyy statisticheskiy test dlya sluchaynykh chisel ["Book Stack" as a new statistical test for random numbers]. Probl. Peredachi Inf., 2004, vol. 40, iss. 1, pp. 73–78. (in Russian)
11. *Ryabko B. Ya., Monarev V. A., and Shokin Yu. I.* Novyy tip atak na blokovye shifry [A new type of attacks on block ciphers]. Probl. Peredachi Inf., 2005, vol. 41, iss. 4, pp. 97–107. (in Russian)
12. *Lysyak A. S., Ryabko B. Ya., and Fionov A. N.* Analiz effektivnosti gradientnoy statisticheskoy ataki na blokovye shifry RC6, MARS, CAST-128, IDEA, Blowfish v sistemakh zashchity informatsii [Efficiency analysis of gradient statistical attack on block ciphers RC6, MARS, CAST-128, IDEA, Blowfish]. Vestnik SibGUTI, 2013, no. 1, pp. 85–109. (in Russian)
13. *Pestunov A. I.* Predvaritel'naya otsenka minimal'nogo chisla raundov legkovesnykh shifrov dlya obespecheniya ikh udovletvoritel'nykh statisticheskikh svoystv [Preliminary evaluation of a minimal number of rounds in lightweight block ciphers for providing their satisfactory statistical properties]. Prikl. Diskr. Mat. Suppl., 2015, iss. 8, pp. 66–68. (in Russian)
14. *Pestunov A. I.* Teoreticheskoe issledovanie svoystv statisticheskogo testa «stopka knig» [Theoretical investigation of the Bookstack test features]. Vychislitel'nye tekhnologii, 2006, vol. 11, no. 6, pp. 96–103. (in Russian)