УДК 621.391:519.2

А. Н. Алексейчук, А. С. Шевцов
Специальный факультет СБ Украины в составе Военного института телекоммуникаций и информатизации НТУУ «КПИ»

Показатели и оценки стойкости блочных шифров относительно статистических атак первого порядка

Получены аналитические верхние оценки надежности различающей и, соответственно, «вскрывающей» статистической атаки первого порядка на блочные шифры. Указанные оценки позволяют ввести теоретически обоснованные показатели стойкости блочных шифров относительно обобщенного линейного, билинейного и ряда других методов криптоанализа. В случае линейной различающей атаки полученная оценка стойкости блочных шифров является более точной по сравнению с ранее известной.

Ключевые слова: *криптографическая защита информации, блочный шифр, обоснованная стойкость, статистическая атака, статистический критерий.*

Введение

Одной из центральных проблем современной симметричной криптографии является создание общей теории обоснования стойкости блочных шифров. Разнообразие существующих методов их криптоанализа, появление новых перспективных направлений в этой области [1] требуют систематизации, упорядочения и осмысления с единых, общих позиций накопленных фактов и отдельных теоретических результатов. Отметим работы [2, 3], в которых представлены концептуальные подходы к обоснованию стойкости блочных шифров на основе понятий различающей атаки, декорреляции и, соответственно, стохастической коммутативной диаграммы.

Несмотря на повышенное внимание специалистов к проблеме теоретического обоснования эффективности известных статистических методов криптоанализа блочных шифров [2–6], эти методы, в подавляющем большинстве, остаются полуэвристическими, «работающими» на практике, но не имеющими строгого обоснования. К их числу относятся классические методы дифференциального и линейного криптоанализа, а также их многочисленные обобщения [1, 3, 7–10], в частности, предложенный недавно метод билинейного криптоанализа шифров Фейстеля

© А. Н. Алексейчук, А. С. Шевцов

[11]. Отсутствие строгости в обосновании известных оценок надежности (вероятности правильного восстановления ключа) или сложности (необходимого числа открытых сообщений) указанных статистических методов связано, прежде всего, с использованием, в явном или неявном виде, различных эвристических или упрощающих предположений, наподобие гипотез «о стохастической эквивалентности», «строгой различимости ключей» и др. [8–10, 12, 13]. Как отмечено в [13] (стр. 414), проверить эти предположения для реальных криптосхем практически невозможно; кроме того, обычно несложно построить пример криптосистемы, для которой рассматриваемое предположение не выполнено. Безукоризненно строгое обоснование условий, обеспечивающих стойкость блочных шифров относительно различающих атак, предложено в [2]. Вместе с тем, модель различающей атаки является несколько ограничительной, и результаты [2] непосредственно не применимы к решению задач оценки или обоснования стойкости блочных шифров относительно практических («вскрывающих») атак.

Целью настоящей статьи является построение теоретически обоснованных верхних оценок надежности статистических (различающей и «вскрывающей») атак первого порядка на блочные шифры. (Согласно [2, 3], атаками первого порядка называются атаки на основе известных или подобранных открытых сообщений, при которых для получения очередной «порции» информации о ключе криптоаналитику достаточно зашифровать ровно одно сообщение. Примерами служат атаки, основанные на методах линейного, обобщенного линейного, билинейного криптоанализа или методе криптоанализа на основе разбиений [7–11]. Дифференциальному криптоанализу соответствуют атаки второго порядка, поскольку в этом случае зашифрованию подвергаются определенные пары открытых сообщений). Полученные оценки позволяют ввести показатели стойкости блочных шифров относительно указанных атак (методов криптоанализа), не прибегая к каким-либо эвристическим или упрощающим предположениям. Для случая линейной различающей атаки получена новая оценка стойкости блочных шифров (сложности атаки), которая оказывается на один–два порядка точнее ранее известной оценки [2].

Постановка задачи

Обозначим S^{V_n} симметрическую группу подстановок на множестве $V_n = \{0,1\}^n$. Зафиксируем отличную от константы булеву функцию $\varphi : V_n \times V_n \to \{0,1\}$. Для любой подстановки $c \in S^{V_n}$ обозначим $I_c(X)$ индикатор события $\{\varphi(X, c(X)) = 0\}$, где X — случайный равновероятный двоичный вектор длины n. По определению $I_c(X) = 1$, если $\varphi(X, c(X)) = 0$; $I_c(X) = 0$ — в противном случае. Положим:

$$p_c = \mathbf{P}\{I_c(X) = 1\},\ \lambda_c = (2p_c - 1)^2,\ c \in S^{V_n}.$$

Для любого множества $N \subseteq S^{V_n}$ обозначим символом $\overline{\lambda}_N$ среднее значение λ_c по всем $c \in N$: $\overline{\lambda}_N = |N|^{-1} \sum_{c \in N} \lambda_c$.

Рассмотрим произвольный блочный шифр $\mathfrak{R}$ с множеством открытых (шифрованных) сообщений V_n, множеством ключей K и семейством шифрующих преобразований $\Lambda = (f_k : k \in K)$. Различающая атака на шифр $\mathfrak{R}$, основанная на отображении φ, осуществляется при следующих вероятностных предположениях [2]. Вначале с вероятностью $1/2$ выбирается число $\nu \in \{0,1\}$. Затем фиксируется значение случайной подстановки C, которая распределена равномерно на всей симметрической группе S^{V_n}, если $\nu = 0$, и совпадает с вероятностью $|K|^{-1}$ с любой из подстановок f_k, $k \in K$, если $\nu = 1$. (Другими словами при $\nu = 0$ C — случайная равновероятная подстановка на множестве V_n, а при $\nu = 1$ C — случайное и равновероятное шифрующее преобразование данного шифра $\mathfrak{R}$). Атака состоит в проведении t независимых испытаний, в i-м из которых криптоаналитик генерирует случайный вектор X_i с равномерным распределением на множестве V_n и вычисляет значение случайной величины:

$$\xi_i = I_C(X_i) = I\{\varphi(X_i, C(X_i)) = 0\},\ i \in \overline{1,t}. \tag{1}$$

При этом предполагается, что случайные векторы $X_1, ..., X_t$ не зависят от случайной подстановки C. Целью атаки является проверка по наблюдаемой реализации случайной последовательности

$$\xi^{(t)} = \xi_1, ..., \xi_t \tag{2}$$

статистической гипотезы $H_0 : \nu = 0$ относительно альтернативы $H_1 : \nu = 1$.

Итак, описанная атака состоит в том, чтобы отличить по результатам зашифрования t открытых сообщений $X_1, ..., X_t$ (на основе информации, содержащейся в реализации случайной последовательности (2)) данный шифр $\mathfrak{R}$ от случайной равновероятной подстановки на множестве V_n. В соответствии с терминологией [2], указанная атака относится к классу неадаптивных различающих атак первого порядка на блочный шифр $\mathfrak{R}$. В частном случае, когда функция φ имеет вид $\varphi(x, y) = g(x) \oplus h(y)$, $(x, y) \in V_n^2$, где $g,\ h : V_n \to \{0,1\}$ — уравновешенные булевы функции, эта атака может быть названа обобщенной линейной [9] (в частности, если g и h — ненулевые линейные булевы функции, то это — классическая линейная различающая атака на шифр $\mathfrak{R}$ [2, 3, 5]). В случае, когда $\mathfrak{R}$ является шифром Фейстеля, $\varphi(x, y) = g(x) \oplus h(y)$ и $g(x) = h(x) = x_1 A x_2^{\mathrm{T}}$, $x = (x_1, x_2) \in V_n$, $x_1,\ x_2 \in V_m$, где $n = 2m$, A — обратимая матрица порядка m над полем $\mathbf{GF}(2)$,

получаем билинейную различающую атаку [11]. Стойкость шифра $\mathfrak{R}$ относительно описанной атаки характеризуется предпочтением (advantage) оптимального статистического критерия для проверки гипотезы H_0 против альтернативы H_1 [2, 5].

Заметим, что различающую атаку нетрудно модифицировать таким образом, чтобы получить «вскрывающую» статистическую атаку на блочный шифр $\mathfrak{R}$. Эта «вскрывающая» атака проводится на основе выбираемых открытых сообщений и использует, помимо указанной выше булевой функции φ, уравновешенную функцию $\psi : K \to \{0,1\}$.

Пусть $k \in K$ — неизвестный ключ шифра $\mathfrak{R}$, выбранный с вероятностью $|K|^{-1}$ из множества K. При проведении атаки криптоаналитик генерирует t независимых, случайных и равновероятных открытых сообщений $X_1, ..., X_t$, зашифровывает их на ключе k и вычисляет значения случайных величин (1), где C обозначает случайное и равновероятное шифрующее преобразование шифра $\mathfrak{R}$. Цель атаки состоит в том, чтобы восстановить значение $\psi(k)$, то есть проверить по наблюдаемой реализации случайной последовательности (2) справедливость гипотезы $H_0 : \text{ш}(K) = 0$ относительно альтернативы $H_1 : \text{ш}(K) = 1$.

Основная задача, решаемая в данной статье, заключается в нахождении аналитических выражений верхних границ предпочтения оптимального критерия для проверки гипотез H_0 и H_1 (как для различающей, так и для «вскрывающей» атак), явно зависящих от шифра $\mathfrak{R}$ и функции φ.

Вспомогательные сведения о статистических критериях для проверки простых гипотез

Пусть N — произвольное конечное множество, $\mathbf{P}_0$ и $\mathbf{P}_1$ — распределения вероятностей на N, ξ — случайная величина, закон распределения которой с вероятностью $1/2$ может быть равен $\mathbf{P}_0$ или $\mathbf{P}_1$. Рассмотрим две гипотезы относительно распределения случайной величины ξ: H_0: ξ распределена по закону $\mathbf{P}_0$; H_1: ξ распределена по закону $\mathbf{P}_1$.

Статистический критерий для проверки гипотезы H_0 против альтернативы H_1 определяется критическим множеством A, состоящим из тех и только тех значений случайной величины ξ, при реализации (наблюдении) каждого из которых гипотеза H_0 отвергается. Средняя вероятность ошибки $P_{e,A}$ критерия, основанного на критическом множестве A, определяется по формуле:

$$P_{e,A} = 1/2\,(\mathbf{P}_0(\xi \in A) + \mathbf{P}_1(\xi \notin A)). \qquad (3)$$

Число

$$\pi_A = |\,2P_{e,A} - 1\,| = |\,\mathbf{P}_0(\xi \in A) - \mathbf{P}_1(\xi \in A)\,| \qquad (4)$$

называется предпочтением данного критерия [2], а число $1 - P_{e,A}$ — его надежностью [13]. Известно (см., например, [13]), что оптимальным (в смысле минимума значений (3) или, что тоже самое, максимума значений (4)) критерием различия гипотез H_0 и H_1 является байесовский критерий, критическое множество A^* которого состоит их тех и только тех значений a случайной величины ξ, которые удовлетворяют неравенству $\mathbf{P}_0(\xi = a) < \mathbf{P}_1(\xi = a)$. Ясно, что средняя вероятность ошибки байесовского критерия $P_{e,A^*} \le 1/2$, то есть $\pi_{A^*} = 1 - 2P_{e,A^*}$.

Рассмотрим задачу проверки гипотез H_0 и H_1 в частном случае, когда ξ принимает значения во множестве V_t двоичных векторов длины t, а распределения $\mathbf{P}_0$ и $\mathbf{P}_1$ имеют следующий вид:

$$\mathbf{P}_0(a) = p^{s(a)}(1-p)^{t-s(a)},\ \mathbf{P}_1(a) = 2^{-t},\ a = (a_1,...,a_t) \in V_t,$$

где $p \in [0,1]$ — фиксированное число; $s(a) = a_1 + ... + a_t$. В этом случае ξ представляет собой последовательность t независимых случайных величин, принимающих значения во множестве $\{0,1\}$ и распределенных по закону Бернулли с параметром p при условии справедливости гипотезы H_0, и по равномерному закону — при условии справедливости гипотезы H_1. Обозначим

$$\pi^*(p;t) = \max_{A \subseteq V_t} \left| \sum_{a \in A} (p^{s(a)}(1-p)^{t-s(a)} - 2^{-t}) \right| \tag{5}$$

предпочтение оптимального (байесовского) критерия для проверки указанных гипотез. В работе [2] (см. доказательство леммы 15) получено следующее утверждение.

Лемма 1. Для любых $p \in [0,1]$, $t \in \mathbf{N}$ справедливо неравенство:

$$\pi^*(p;t) \le 2\sqrt{t}\,|2p-1|. \tag{6}$$

Из формулы (6) вытекает следующая верхняя граница надежности оптимального критерия для проверки гипотез H_0 и H_1:

$$1 - P_{e,A^*} \le 1/2 + \sqrt{t}\,|2p-1|. \tag{7}$$

Отметим, что в [2] приведены условия, при которых оценки (6), (7) являются неулучшаемыми по порядку величины.

Оценки стойкости блочных шифров относительно представленных статистических атак

Получим верхнюю границу предпочтения $\pi^*(\Re,\varphi)$ оптимального критерия для проверки по наблюдаемой реализации случайной последовательности (2) двух простых гипотез: H_0 — случайная подстановка C имеет равномерное распределение на множестве S^{V_n}; H_1 — эта подстановка является случайным и равновероятным шифрующим преобразованием блочного шифра $\Re$. С этой целью найдем апостериорное распределение вероятностей случайной последовательности $\xi^{(t)}$ при условии справедливости каждой из указанных гипотез.

Обозначим $\mathbf{P}_\nu(a) = \mathbf{P}(\xi^{(t)} = a \mid H_\nu)$, $a \in V_t$, $\nu \in \{0,1\}$. Используя введенные выше обозначения, получим:

$$\mathbf{P}_0(a) = |S^{V_n}|^{-1} \sum_{c\in S^{V_n}} \mathbf{P}\{I_c(X_1) = a_1,\ldots, I_c(X_t) = a_t\} = |S^{V_n}|^{-1} \sum_{c\in S^{V_n}} \prod_{i=1}^{t} p_c^{a_i}(1-p_c)^{1-a_i} =$$
$$= |S^{V_n}|^{-1} \sum_{c\in S^{V_n}} p_c^{s(a)}(1-p_c)^{t-s(a)}, \qquad (8)$$

где $s(a) = a_1 + \ldots + a_t$, $a = (a_1,\ldots,a_t) \in V_t$. Аналогично найдем:

$$\mathbf{P}_1(a) = |K|^{-1} \sum_{k\in K} p_{f_k}^{s(a)}(1-p_{f_k})^{t-s(a)}, \; a \in V_t. \qquad (9)$$

Отсюда, согласно формуле (4), получим:

$$\pi^*(\Re,\varphi) = \left|\sum_{a\in A^*} \mathbf{P}_0(a) - \sum_{a\in A^*} \mathbf{P}_1(a)\right| \le \left|\sum_{a\in A^*} (\mathbf{P}_0(a) - 2^{-t})\right| + \left|\sum_{a\in A^*} (\mathbf{P}_1(a) - 2^{-t})\right|, \qquad (10)$$

где A^* — критическое множество оптимального критерия различения сформулированных выше гипотез H_0 и H_1.

Оценим сверху каждое из двух слагаемых в правой части неравенства (10). Имеем:

$$\sigma_0^*(\Re,\varphi) \overset{\text{def}}{=} \left|\sum_{a\in A^*} (P_0(a) - 2^{-t})\right| = \left||S^{V_n}|^{-1} \sum_{c\in S^{V_n}} \sum_{a\in A^*} (p_c^{s(a)}(1-p_c)^{t-s(a)} - 2^{-t})\right| \le$$
$$\le |S^{V_n}|^{-1} \sum_{c\in S^{V_n}} \left|\sum_{a\in A^*} (p_c^{s(a)}(1-p_c)^{t-s(a)} - 2^{-t})\right|.$$

Отсюда на основании формул (5), (6) заключаем, что

$$\sigma_0^*(\Re,\varphi) \le |S^{V_n}|^{-1} \sum_{c\in S^{V_n}} 2\sqrt{t}\,|2p_c - 1| = 2\sqrt{t}\,|S^{V_n}|^{-1} \sum_{c\in S^{V_n}} \sqrt{\lambda_c} \le$$

$$\le 2\sqrt{t}\left(\sum_{c\in S^{V_n}} |S^{V_n}|^{-1}\,\lambda_c\right)^{1/2} = 2\sqrt{t}\,(\overline{\lambda}_{S^{V_n}})^{1/2}, \qquad (11)$$

где последнее неравенство следует из выпуклости вверх функции $\sqrt{x}$, $x \ge 0$. Аналогично получаем:

$$\sigma_1^*(\Re,\varphi) \stackrel{\text{def}}{=} \left|\sum_{a\in A^*} (\mathbf{P}_1(a) - 2^{-t})\right| \le 2\sqrt{t}\,(\overline{\lambda}_\Lambda)^{1/2} = 2\sqrt{t}\left(|K|^{-1} \sum_{k\in K} \lambda_{f_k}\right)^{1/2}. \qquad (12)$$

Складывая неравенства (11), (12), в силу соотношения (10), получим следующую оценку:

$$\pi^*(\Re,\varphi) \le 2\sqrt{t}\left((\overline{\lambda}_{S^{V_n}})^{1/2} + (\overline{\lambda}_\Lambda)^{1/2}\right). \qquad (13)$$

Лемма 2. Для любой уравновешенной функции $\varphi : V_n \times V_n \to \{0,1\}$ справедливы равенства:

$$\overline{\lambda}_{S^{V_n}} = |S^{V_n}|^{-1} \sum_{c\in S^{V_n}} (2\mathbf{P}\{\varphi(X, c(X)) = 0\} - 1)^2 =$$

$$= (2^n - 1)^{-1} - 2^{-n}(2^n - 1)^{-1} 2^{-2n} \sum_{(x,x')\in V_n^2} (-1)^{\varphi(x,x')} \left(\sum_{y\in V_n} (-1)^{\varphi(y,x')} + \sum_{y'\in V_n} (-1)^{\varphi(x,y')}\right). \qquad (14)$$

В частности, если для любого $x \in V_n$ функции $\varphi(x, \cdot)$ и $\varphi(\cdot, x)$ являются уравновешенными, то

$$\overline{\lambda}_{S^{V_n}} = (2^n - 1)^{-1}. \qquad (15)$$

Доказательство. На основании формулы

$$2\mathbf{P}\{\varphi(X, c(X)) = 0\} - 1 = 2^{-n} \sum_{x\in V_n} (-1)^{\varphi(x,c(x))},\ c \in S^{V_n},$$

справедливы равенства:

$$\overline{\lambda}_{S^{V_n}} = 2^{-2n} \sum_{c\in S^{V_n}} |S^{V_n}|^{-1} \sum_{(x,y)\in V_n^2} (-1)^{\varphi(x,c(x)) \oplus \varphi(y,c(y))} =$$

$$2^{-n} + 2^{-2n} \mid S^{V_n} \mid^{-1} \sum_{c \in S^{V_n}} \sum_{\substack{(x,y) \in V_n^2: \\ x \neq y}} (-1)^{\varphi(x, c(x))} (-1)^{\varphi(y, c(y))} =$$

$$= 2^{-n} + 2^{-2n} \mid S^{V_n} \mid^{-1} \sum_{\substack{(x,y),(x',y') \in V_n: \\ x \neq y,\, x' \neq y'}} \mid \{c \in S^{V_n} : c(x) = x', c(y) = y'\} \mid (-1)^{\varphi(x,x')} (-1)^{\varphi(y,y')} =$$

$$= 2^{-n} + 2^{-n} (2^n - 1)^{-1} 2^{-2n} \sum_{(x',x) \in V_n} (-1)^{\varphi(x,x')} \sum_{\substack{(y,y') \in V_n^2: \\ x \neq y,\, x' \neq y'}} (-1)^{\varphi(y,y')}. \qquad (16)$$

Заметим теперь, что в силу уравновешенности функции φ:

$$\sum_{\substack{(y,y') \in V_n^2: \\ x \neq y,\, x' \neq y'}} (-1)^{\varphi(y,y')} = -\left(\sum_{y \in V_n} (-1)^{\varphi(y,x')} + \sum_{y' \in V_n} (-1)^{\varphi(x,y')} - (-1)^{\varphi(x,x')} \right),$$

откуда в силу соотношений (16) вытекает равенство (14). Лемма доказана.

Итак, на основании неравенства (13) и утверждения леммы 2 справедлива следующая теорема, устанавливающая верхнюю границу параметра $\pi^*(\Re, \varphi)$.

Теорема 1. Пусть $\varphi(x, y) = g(x) \oplus h(y)$, $(x, y) \in V_n^2$, где $g,\ h : V_n \to \{0,1\}$ — уравновешенные булевы функции, $\pi^*(\Re, \varphi)$ — предпочтение оптимального критерия для проверки гипотез H_0 и H_1 по реализации случайной последовательности (2) (в случае различающей атаки на блочный шифр $\Re$). Тогда справедливо неравенство:

$$\pi^*(\Re, \varphi) \le 2\sqrt{t}\left((\bar{\lambda}_\Lambda)^{1/2} + (2^n - 1)^{-1/2} \right), \qquad (17)$$

где

$$\bar{\lambda}_\Lambda = \mid K \mid^{-1} \sum_{k \in K} (2\mathbf{P}\{\varphi(X, f_k(X)) = 0\} - 1)^2. \qquad (18)$$

Получим теперь верхнюю оценку предпочтения $\pi^*(\Re; \varphi, \text{ш})$ оптимального критерия различения гипотез $H_0 : \text{ш}(K) = 0$ и $H_1 : \text{ш}(K) = 1$, соответствующих описанной выше «вскрывающей» атаке на шифр $\Re$. Обозначим A^* критическое множество указанного критерия, $\mathbf{P}_\nu(a) = \mathbf{P}(\xi^{(t)} = a \mid H_\nu)$ — апостериорную вероятность реализации $a = (a_1, \ldots, a_t) \in V_t$ случайной последовательности (2) при условии справедливости гипотезы H_ν, $\nu \in \{0, 1\}$. Положим $p_k = \mathbf{P}\{I_{f_k}(X) = 1\}$, $\lambda_k = (2p_k - 1)^2$, $k \in K$.

В силу уравновешенности функции ψ справедливо равенство:

$$\mathbf{P}_\nu(a)=\frac{2}{|K|}\sum_{\substack{k\in K:\\ \psi(K)=\nu}} p_k^{a_1}(1-p_k)^{1-a_1}\cdots p_k^{a_t}(1-p_k)^{1-a_t}=\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(K)=\nu}} p_k^{s(a)}(1-p_k)^{t-s(a)}.$$

Следовательно, согласно формуле (4),

$$\pi^*(\mathfrak{R};\varphi,\psi)=\left|\sum_{a\in A^*}(\mathbf{P}_0(a)-\mathbf{P}_1(a))\right|\le\left|\sum_{a\in A^*}(\mathbf{P}_0(a)-2^{-t})\right|+\left|\sum_{a\in A^*}(\mathbf{P}_1(a)-2^{-t})\right|, \qquad (19)$$

$$\left|\sum_{a\in A^*}(\mathbf{P}_\nu(a)-2^{-t})\right|=\left|\sum_{a\in A^*}\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=\nu}}(p_k^{s(a)}(1-p_k)^{t-s(a)}-2^{-t})\right|\le$$

$$\le\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=\nu}}\left|\sum_{a\in A^*}(p_k^{s(a)}(1-p_k)^{t-s(a)}-2^{-t})\right|\le 2\sqrt{t}\left(\frac{|K|}{2}\right)^{-1}\sum_{\substack{k\in K:\\ \psi(k)=\nu}}\lambda_k^{1/2},\ \nu\in\{0,1\}, \qquad (20)$$

где последнее неравенство вытекает из леммы 1.

Складывая оценки (20) при $\nu=0$ и $\nu=1$, на основании соотношений (19) и выпуклости вверх функции $\sqrt{x}$, $x\ge 0$, получим:

$$\pi^*(\mathfrak{R};\varphi,\text{ш})\le 2\sqrt{t}\left(\sum_{k\in K}\lambda_k^{1/2}\right)2\,|K|^{-1}\le 4\sqrt{t}\left(|K|^{-1}\sum_{k\in K}\lambda_k\right)^{1/2}.$$

Итак, доказана следующая теорема.

Теорема 2. Пусть $\pi^*(\mathfrak{R};\varphi,\text{ш})$ — предпочтение оптимального критерия для проверки гипотез $H_0:\text{ш}(K)=0$ и $H_1:\text{ш}(K)=1$ по реализации случайной последовательности (2) (в случае «вскрывающей» атаки на шифр $\mathfrak{R}$). Тогда справедливо неравенство:

$$\pi^*(\mathfrak{R};\varphi,\text{ш})\le 4\sqrt{t}\,(\overline{\lambda}_\Lambda)^{1/2}, \qquad (22)$$

где $\overline{\lambda}_\Lambda$ определяется по формуле (18).

Отметим, что в приведенном доказательстве теоремы 2 не используются какие-либо эвристические предположения (вроде гипотез «о стохастической эквивалентности» или «строгой различимости ключей» [8–10, 12, 13]) относительно шифра $\mathfrak{R}$.

Обсуждение полученных результатов

Соотношения (17) и (22) устанавливают верхние границы стойкости произвольного блочного шифра относительно описанных выше (соответственно, разли-

чающей и «вскрывающей») статистических атак. Эти соотношения позволяют ввести (обоснованно, не прибегая к эвристическим рассуждениям) показатели стойкости блочных шифров относительно известных методов криптоанализа (обобщенного линейного [9], билинейного [11]), а также их возможных обобщений. Как следует из описаний статистических атак на шифр $\Re$, каждый из указанных криптоаналитических методов определяется выбором функции φ из подходящего класса булевых функций $2n$ переменных. При этом параметр, характеризующий стойкость шифра $\Re$ к данному методу криптоанализа, определяется по формуле (18). Отметим, что в частном случае, когда φ является линейной булевой функцией, «вскрывающая» атака на шифр $\Re$ близка к так называемому Алгоритму 1, предложенному М. Матцуи [8], а параметр (18) совпадает с классическим показателем стойкости блочных шифров относительно метода линейного криптоанализа [14].

Для линейной различающей атаки на шифр $\Re$ в [2] получена верхняя граница предпочтения $\pi^*(\Re,\varphi)$, которая имеет следующий вид:

$$\pi^*(\Re,\varphi) \le 3\sqrt[3]{t}\,((\overline{\lambda}_\Lambda)^{1/3} + (2^n-1)^{-1/3}). \qquad (23)$$

Заметим, что в случае, когда оценка (23) является нетривиальной (то есть выражение в правой части неравенства (23) не превосходит 1), она оказывается более грубой по сравнению с оценкой (17). Ниже, в таблице приведены численные значения параметра $t\,\overline{\lambda}_\Lambda$, характеризующего сложность линейной различающей атаки на шифр $\Re$, при различных значениях надежности $N(\Re,\varphi) = 0{,}5(1+\pi^*(\Re,\varphi))$, полученные с использованием неравенств (17) и (23). (Данные в таблице рассчитаны по формулам $t\,\overline{\lambda}_\Lambda \ge 1/4\,(N(\Re,\varphi)-0{,}5)^2$ и $t\,\overline{\lambda}_\Lambda \ge 1/27\,(N(\Re,\varphi)-0{,}5)^3$, вытекающим из неравенств (17) и (23) соответственно, а также известного неравенства $\overline{\lambda}_\Lambda \ge (2^n-1)^{-1}$; см., например, лемму 1 в [15]).

Сравнение оценок сложности различающей линейной атаки на блочные шифры

Надежность атаки	Неравенство (17)	Неравенство (23)
0,9	0,04000	0,00237
0,8	0,02250	0,00100
0,7	0,01000	0,00029
0,6	0,00250	0,00004

Как видно из таблицы, оценка сложности атаки, полученная с использованием формулы (17), примерно на один–два порядка точнее оценки, вытекающей из формулы (23). (Например, согласно неравенству (23), для того, чтобы отличить шифр $\Re$ от случайной равновероятной подстановки с надежностью 0,9, требуется зашифровать не менее $0{,}00237(\overline{\lambda}_\Lambda)^{-1}$ открытых сообщений. В то же время, со-

гласно неравенству (17), для этого необходимо не менее $0{,}04000\,(\overline{\lambda}_{\Lambda})^{-1}$ открытых сообщений).

В целом, полученные результаты составляют теоретическую основу для дальнейших исследований в области анализа и обоснования стойкости блочных шифров относительно статистических атак первого порядка, позволяя сосредоточить основные усилия на разработке методов построения нетривиальных верхних границ параметров вида (18).

1. *Biryukov A.* Block Ciphers and Stream Ciphers: the State of the Art // http://eprint.iacr.org/2004/094.

2. *Vaudenay S.* Decorrelation: a Theory for Block Cipher Security // J. of Cryptology. — 2003. — Vol. 16, N 4. — P. 249–286.

3. *Wagner D.* Towards a Unifying View of Block Cipher Cryptanalysis // Fast Software Encryption. — FSE'04, Proceedings. — Springer Verlag, 2004. — P. 116–135.

4. *Vaudenay S.* On the Security of CS-Cipher // Fast Software Encryption. — FSE'99, Proceedings. — Springer Verlag, 1999. — P. 260–274.

5. *Junod P.* On the Optimality of Linear, Differential and Sequential Distinguishers // Advances in Cryptology — EUROCRYPT'03 — Springer Verlag, 2003. — P. 17–32.

6. *Baigneres T.*, *Vaudenay S.* Proving the Security of AES Substitution-Permutation Network // http://lasecwww.eptf.ch./php_code/publications.

7. *Biham E*, *Shamir A.* Differential Cryptanalysis of DES-Like Cryptosystems // J. of Cryptology. — 1991. — Vol. 4, N 1. — P. 3–72.

8. *Matsui M.* Linear Cryptanalysis Methods for DES Cipher // Advances in Cryptology — EUROCRYPT'93, Proceedings. — Springer Verlag, 1994. — P. 386–397.

9. *Harpes C.*, *Kramer G.G.*, *Massey J.L.* A Generalization of Linear Cryptanalysis and the Applicability of Matsui's Piling-up Lemma // Advances in Cryptology — EUROCRYPT'95, Proceedings. — Springer Verlag, 1995. — P. 24–38.

10. *Harpes C.*, *Massey J.L.* Partitioning Cryptanalysis // Fast Software Encryption. — FSE'97, Proceedings. — Springer Verlag, 1997. — P. 13–27.

11. *Courtois N.T.* Feistel Schemes and Bi-Linear Cryptanalysis // Advances in Cryptology — CRYPTO'04, Proceedings. — Springer Verlag, 2004. — P. 23–40.

12. *Junod P.* On the Complexity of Matsui's Attack // Fast Software Encryption. — FSE'01, Proceedings. — Springer Verlag, 2001. — P. 199–211.

13. *Логачев О.А.*, *Сальников А.А.*, *Ященко В.В.* Булевы функции в теории кодирования и криптологии. — М.: МЦНМО, 2004. — 470 с.

14. *Chabaud F.*, *Vaudenay S.* Links Between Differential and Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT'94, Proceedings. — Springer Verlag, 1995. — P. 356–365.

15. *Keliher L.*, *Meier H.*, *Tavares S.* Improving the Upper Bond on the Maximum Average Linear Hull Probability for Rijndael // Selected Areas in Cryptography. — SAC 2001. — Proceedings. — Springer Verlag, 2001. — P. 112–128.

Поступила в редакцию 08.12.2006