Math-Net.Ru

Общероссийский математический портал

В. А. Федченко, О линейном и разностном криптоанализе AES-подобных алгоритмов шифрования, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 3, 101–120

DOI: <https://doi.org/10.4213/mvk334>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.92.164.108

26 апреля 2023 г., 16:57:09

О линейном и разностном криптоанализе AES-подобных алгоритмов шифрования

В. А. Федченко

Белорусский государственный университет, Минск, Беларусь

Получено 31.V.2019

Аннотация. На примерах AES-подобных алгоритмов шифрования систематически изложен один известный подход к линейному и разностному методам криптографического анализа. Получены новые результаты, позволяющие уточнять показатели рассеивания, важные с точки зрения применения линейного и разностного методов. Приводимые примеры иллюстрируют недостатки общепринятых оценок стойкости.

Ключевые слова: AES, AES-подобный алгоритм, XSLP-шифр, линейный криптоанализ, разностный криптоанализ, активный S-блок, коэффициент рассеивания

On the linear and differential cryptanalysis of the AES-like ciphers

V. A. Fedchenko

Belarusian State University, Minsk, Belarus

Abstract. In the context of AES-like ciphers we give an outline of specific approach to linear and differential cryptanalysis. We obtain new results permitting to improve estimates of important linear and differential characteristics of AES-like ciphers. Some examples illustrates drawbacks in conventional proofs of security.

Keywords: AES, AES-like algorithm, XSLP-cipher, linear cryptanalysis, differential cryptanalysis, active *S*-box, branch number, linear (differential) trail

В последнее время в [1–4] был представлен хорошо разработанный взгляд на линейный [15] и разностный [8] методы криптографического анализа. Этот взгляд имеет существенные отличия от общепринятого, в котором кульминацией можно считать работу по обоснованию стойкости алгоритма шифрования AES [10]. При альтернативном подходе предлагается рассматривать линейный и разностный методы без излишней опоры на предположения или гипотезы. Во всех случаях проводятся обоснованные границы между реальными величинами и оценками для них, эмпирическими данными и теоретическими аппроксимациями. Этот взгляд позволяет вернуться к проблеме обоснования линейного и разностного методов, которая не может считаться решенной по крайней мере в рамках теоретической криптографии. Основываясь на данной методологии, автор рассматривает в настоящей работе отдельные вопросы применения линейного и разностного методов криптографического анализа к AES-подобным алгоритмам шифрования.

В разделах 1–4 кратко изложена теория локального линейного и разностного методов, предлагаемая в работах [1–4]. Раздел 5 в терминах работы [5] содержит используемые далее известные результаты по оценке стойкости AES-подобных алгоритмов шифрования, связанные с показателями рассеивания линейной среды. В разделе 6 вводятся новые характеристики для оценки рассеивающих свойств шифрпреобразований. В разделе 7 предложен метод вычисления коэффициентов рассеивания обратимых линейных преобразований. В разделе 8 представлен подход к уточнению нижних оценок для показателей рассеивания линейной среды AES-подобных алгоритмов шифрования на основе результатов раздела 7 и работы [6]. В разделе 9 приведен пример построения линейных соотношений, который иллюстрирует возникающие при этом вопросы, оправдывающие излагаемую в работе точку зрения.

1. Функциональные схемы отображений векторных пространств. Напомним основные определения и обозначения, принятые в работах [1–4]. Пусть $V_n = \text{GF}(2)^n = \{0, 1\}^n$ — пространство двоичных векторов, состоящих из $n \in \mathbb{N}$ битов. Рассмотрим отображение $F: V_N \rightarrow V_M$, $F(a) = b$, $a = (a_1, a_2, \dots, a_N) \in V_N$, $b = (b_1, b_2, \dots, b_M) \in V_M$, $N, M \in \mathbb{N}$, задающее некоторое шифрпреобразование. На практике подобные отображения конструируются из функций, действующих на векторах относительно небольшой размерности. В связи с этим отображение F удобно задавать с помощью *функциональной схемы* [1], состоящей из некоторого количества функциональных элементов. Каждый *функциональный элемент* представляет собой

отображение, связывающее входные и выходные биты по определенному правилу. В функциональной схеме любой выход (вход) одного функционального элемента может быть единственным образом соединен с входом (выходом) другого функционального элемента направленной связью, действующей от выхода к входу. При этом в функциональной схеме не допускаются циклы из направленных связей. Свободные входы и выходы функциональных элементов в совокупности образуют соответственно вход и выход функциональной схемы. Таким образом, вычисление значения отображения F сводится к вычислению значений функциональных элементов в порядке определения их аргументов, что может быть реализовано в виде компьютерной программы без циклов.

Очевидно, что задание произвольного отображения F в виде функциональной схемы не является однозначным. Вместе с тем предполагается, что такое задание зафиксировано и отображение рассматривается в контексте конкретной функциональной схемы, которую в этом случае обозначают $\mathcal{F}$.

В функциональной схеме $\mathcal{F}$ можно выделить нелинейные (общего вида) и линейные функциональные элементы. *Нелинейные* функциональные элементы в количестве $k \in \mathbb{N}_0$ представляют собой булевы вектор-функции $f_i : V_{n_i} \rightarrow V_{m_i}$, $f_i(x_i) = y_i$, $x_i = (x_{i,1}, x_{i,2}, \dots, x_{i,n_i}) \in V_{n_i}$, $y_i = (y_{i,1}, y_{i,2}, \dots, y_{i,m_i}) \in V_{m_i}$, $n_i, m_i \in \mathbb{N}$, $i = 1, 2, \dots, k$. *Линейные* функциональные элементы образуют так называемую *линейную среду* функциональной схемы $\mathcal{F}$. Они устанавливают связь между выходами и входами нелинейных функциональных элементов и функциональной схемы в целом. Ввиду линейности эту связь можно выразить в матричном виде:

$$(a, y_1, y_2, \dots, y_k) \cdot C^{\mathcal{F}} = (x_1, x_2, \dots, x_k, b), \quad (1)$$

где $C^{\mathcal{F}}$ — матрица размеров $(N + \sum_{i=1}^k m_i) \times (M + \sum_{i=1}^k n_i)$ над полем $\text{GF}(2)$, называемая *матрицей линейной среды* функциональной схемы $\mathcal{F}$.

Все рассуждения, приводимые в работе, хорошо иллюстрируются на следующем простом примере.

Пример 1. Рассмотрим отображение $F : V_n \rightarrow V_n$, задающее r итераций *XSLP-схемы* с размером блока $n = mk^2$ битов [2], где $r, m, k \in \mathbb{N}$. Напомним, что i -я итерация *XSLP-схемы* последовательно реализует:

побитовое сложение по модулю 2 входного блока с ключом $z_i \in V_n$,
замену m -векторов (из V_m) в локальных подстановках $\pi_{i,j} \in S(V_m)$,

Рис. 1. Функциональная схема одной итерации XSLP-схемы с размером блока $n = mk^2$ битов при $m = 3$, $k = 2$

нейное вероятностное соотношение для отображения f , записываемое в виде $x \cdot l' \simeq f(x) \cdot l''$ и характеризующееся вероятностью

$$P\{x \cdot l' = f(x) \cdot l''\} = \frac{1 + \delta_{l', l''}^f}{2}, \quad (3)$$

где x выбирается из V_n случайно и равновероятно, а величина $\delta_{l', l''}^f \in [-1, 1]$ называется *линейной характеристикой* (преобладанием) линейного вероятностного соотношения. Нетрудно показать, что

$$\delta_{0,0}^f = 1 \quad \text{и} \quad \delta_{l',0}^f = 0 \quad \text{при} \quad l' \neq 0. \quad (4)$$

В разностном методе пара вектор-строк $d' \in V_n$, $d'' \in V_m$ задает *разностное вероятностное соотношение* для отображения f с соответствующей *разностной характеристикой*

$$p_{d', d''}^f = P\{f(x \oplus d') \oplus f(x) = d''\} \in [0, 1], \quad (5)$$

где x выбирается из V_n случайно и равномерно. Нетрудно показать, что

$$p_{0,0}^f = 1 \quad \text{и} \quad p_{0,d''}^f = 0 \quad \text{при} \quad d'' \neq 0. \quad (6)$$

Наиболее предпочтительным является нахождение таких (*наилучших*) линейных и разностных вероятностных соотношений, для которых достигаются соответствующие максимумы:

$$\delta^f = \max_{\nu \in V_n^*, l'' \in V_m^* \setminus \{0\}} |\delta_{l'', l''}^f| \quad \text{и} \quad d^f = \max_{d' \in V_n \setminus \{0\}, d'' \in V_m} p_{d', d''}^f, \quad (7)$$

где δ^f и p^f — *линейная и разностная характеристики отображения f* .

3. Локальные методы построения линейных и разностных вероятностных соотношений. Нахождение наилучших в указанном выше смысле вероятностных соотношений для шифрпреобразования $F : V_N \rightarrow V_M$ сопряжено со значительными трудностями уже при $N, M \gtrsim 16$. В связи с этим обычно обращаются к функциональной схеме $\mathcal{F}$ с нелинейными функциональными элементами $f_i : V_{n_i} \rightarrow V_{m_i}$ в количестве $k \in \mathbb{N}_0$ при относительно небольших $n_i, m_i \in \mathbb{N}$, $i = 1, 2, \dots, k$. Тогда *глобальные* линейные (L', L'') и разностные (D', D'') вероятностные соотношения для отображения F получают с применением *систем согласованных локальных* линейных (l'_i, l''_i) и разностных (d'_i, d''_i) вероятностных соотношений для отображений f_i соответственно.

Система локальных линейных вероятностных соотношений $\mathfrak{L} = ((l'_i, l''_i), i = 1, 2, \dots, k)$ является согласованной, если при некоторых $L' = L'_\mathfrak{L} \in V_N^*$, $L'' = L''_\mathfrak{L} \in V_M^*$ только из условий (1), причем, что важно, без привлечения равенств $f_i(x_i) = y_i$, $i = 1, 2, \dots, k$, можно получить в виде следствия равенство

$$\sum_{i=1}^k (x_i \cdot l'_i \oplus y_i \cdot l''_i) = a \cdot L' \oplus b \cdot L''. \quad (8)$$

В этом случае величину

$$\tilde{\delta}_\mathfrak{L} = \prod_{i=1}^k \delta_{l'_i, l''_i}^{f_i} \quad (9)$$

обычно рассматривают в качестве приближения для $\delta_{L'_\mathfrak{L}, L''_\mathfrak{L}}^F$ [4]. В [4] показано, что условие (8) равносильно равенству

$$C^\mathcal{F} \cdot \begin{pmatrix} l'_1 \\ \vdots \\ l'_k \\ L'' \end{pmatrix} = \begin{pmatrix} L' \\ l''_1 \\ \vdots \\ l''_k \end{pmatrix}. \quad (10)$$

Система локальных разностных вероятностных соотношений $\mathfrak{D} = ((d'_i, d''_i), i = 1, 2, \dots, k)$ является согласованной, если при некоторых $D' = D'_\mathfrak{D} \in V_N$, $D'' = D''_\mathfrak{D} \in V_M$ выполнено равенство

$$(D', d'_1, \dots, d'_k) \cdot C^{\mathcal{F}} = (d'_1, \dots, d'_k, D''). \quad (11)$$

Условие (11) получено путем сложения равенств вида (1) для двух входов функциональной схемы $a^{(1)}, a^{(2)} \in V_N$, где $D'_\mathfrak{D} = a^{(1)} \oplus a^{(2)}$, $D''_\mathfrak{D} = b^{(1)} \oplus b^{(2)}$, $b^{(j)} = F(a^{(j)})$, $d'_i = x_i^{(1)} \oplus x_i^{(2)}$, $d''_i = y_i^{(1)} \oplus y_i^{(2)}$, $i = 1, 2, \dots, k$, $j = 1, 2$. Обозначения $x_i^{(j)}$ и $y_i^{(j)}$ используются соответственно для входа и выхода функционального элемента f_i при входе функциональной схемы $a^{(j)}$. Величину

$$\tilde{p}_\mathfrak{D} = \prod_{i=1}^k p_{d'_i, d''_i}^{f_i} \quad (12)$$

обычно рассматривают в качестве приближения для $p_{D'_\mathfrak{D}, D''_\mathfrak{D}}^{\mathcal{F}}$ [4].

При рассмотрении линейного и разностного методов важно иметь в виду, что величины $\tilde{\delta}_\mathfrak{D}$ и $\tilde{p}_\mathfrak{D}$ не являются в какой-либо степени доказуемо точными приближениями для соответствующих $\delta_{L'_\mathfrak{D}, L''_\mathfrak{D}}^{\mathcal{F}}$ и $p_{D'_\mathfrak{D}, D''_\mathfrak{D}}^{\mathcal{F}}$. Эксперименты показывают, что иногда действительно имеет место близость по порядку соответствующих величин, вместе с тем существуют примеры и значительных расхождений. Эти и другие важные аргументы о качественных недостатках рассматриваемых приближений приводятся в [4]. Там же впервые представлены теоремы о точных значениях линейной и разностной характеристик для линейных и разностных вероятностных соотношений.

Пусть $\mathcal{L}^{\mathcal{F}}(L', L'')$ и $\mathcal{D}^{\mathcal{F}}(D', D'')$ — множества систем локальных вероятностных соотношений, удовлетворяющих условиям согласованности (10) и (11) при заданных (L', L'') и (D', D'') соответственно.

Теорема 1 (Ф. М. Малышев). Для любых $L' \in V_N^*$, $L'' \in V_M^*$ имеем

$$\delta_{L', L''}^{\mathcal{F}} = \sum_{\mathfrak{L} \in \mathcal{L}^{\mathcal{F}}(L', L'')} \tilde{\delta}_\mathfrak{L}. \quad (13)$$

Теорема 2 (Ф. М. Малышев). Для любых $D' \in V_N$, $D'' \in V_M$ имеем

$$p_{D', D''}^{\mathcal{F}} = \sum_{\mathfrak{D} \in \mathcal{D}^{\mathcal{F}}(D', D'')} \tilde{p}_\mathfrak{D} + \frac{1}{2^M} \sum_{L' \in V_N^*, L'' \in V_M^*} (-1)^{D' L' \oplus D'' L''} \sum_{\substack{\mathfrak{L}_1, \mathfrak{L}_2 \in \mathcal{L}^{\mathcal{F}}(L', L''), \\ \mathfrak{L}_1 \neq \mathfrak{L}_2}} \tilde{\delta}_{\mathfrak{L}_1} \cdot \tilde{\delta}_{\mathfrak{L}_2}. \quad (14)$$

После того как теоремы 1 и 2 сформулированы, они достаточно просто доказываются индукцией по $k \in \mathbb{N}_0$ с помощью техники работы [1], относящейся к линейной среде, и с учетом уже известных доказательств теоремы 1 в частных случаях, которые основаны на следующей лемме.

Лемма 1 ([17]). Пусть $f : V_n \rightarrow V_m$, $f = gh$, т.е. $f(x) = h(g(x))$ для всех $x \in V_n$, где $g : V_n \rightarrow V_t$ и $h : V_t \rightarrow V_m$, $n, m, t \in \mathbb{N}$. Тогда для любых $l' \in V_n^*$, $l'' \in V_m^*$ имеем

$$\delta_{l', l''}^f = \sum_{l \in V_t^*} \delta_{l', l}^g \cdot \delta_{l, l''}^h. \quad (15)$$

Далее приведем только план доказательств, не вдаваясь в излишние детали, поддающиеся непосредственной проверке. Базы индукции проверяются исходя из определений. Индуктивные переходы используют суперпозицию $F = F_1 \cdot F_2$, $F_1 : V_N \rightarrow V_T$, $F_2 : V_T \rightarrow V_M$, где отображения F_i реализуются функциональными схемами $\mathcal{F}_i$, $i = 1, 2$. Для матрицы линейной среды $C^{\mathcal{F}}$ используется ее выражение через $C^{\mathcal{F}_1}$ и $C^{\mathcal{F}_2}$. При этом понятно, что $\mathcal{L}^{\mathcal{F}}(L', L'') = \cup_{L \in V_T^*} (\mathcal{L}^{\mathcal{F}_1}(L', L) \times \mathcal{L}^{\mathcal{F}_2}(L, L''))$, $\mathcal{D}^{\mathcal{F}}(L', L'') = \cup_{D \in V_T} (\mathcal{D}^{\mathcal{F}_1}(D', D) \times \mathcal{D}^{\mathcal{F}_2}(D, D''))$.

Теорема 2 следует из теоремы 1 и следующей леммы.

Лемма 2 ([11]). Пусть $f : V_n \rightarrow V_m$, $n, m \in \mathbb{N}$. Тогда для любых $d' \in V_n$, $d'' \in V_m$ имеем

$$p_{d', d''}^f = \frac{1}{2^m} \sum_{l' \in V_n^*, l'' \in V_m^*} (-1)^{d' \cdot l' \oplus d'' \cdot l''} \left(\delta_{l', l''}^f \right)^2. \quad (16)$$

Применение леммы 2 предполагает доказательство индукцией по $k \in \mathbb{N}_0$ равенства

$$\sum_{\mathfrak{D} \in \mathcal{D}^{\mathcal{F}}(D', D'')} \tilde{p}_{\mathfrak{D}} = \frac{1}{2^M} \sum_{L' \in V_N^*, L'' \in V_M^*} (-1)^{D' \cdot L' \oplus D'' \cdot L''} \sum_{\mathfrak{L} \in \mathcal{L}^{\mathcal{F}}(L', L'')} \tilde{\delta}_{\mathfrak{L}}^2. \quad (17)$$

Заметим, что если $F(a) = G(a \cdot C_1) \oplus a \cdot C_2$, где C_1, C_2 — матрицы размеров $N \times N_1$ и $N \times M$ соответственно, а $G : V_{N_1} \rightarrow V_M$ — отображение, задаваемое функциональной схемой $\mathcal{G}$, то равенство (17) будет следовать из аналогичного равенства, но выписанного не для функциональной схемы $\mathcal{F}$, а для функциональной схемы $\mathcal{G}$. Поэтому при $k = 1$ равенство (17) достаточно доказать при $F(a) = f_1(a) \cdot C$, где C

— матрица размеров $m_1 \times M$, тогда (17) равносильно непосредственно проверяемому равенству (14).

Несмотря на явные недостатки приближений (9) и (12), они находят широкое применение ввиду отсутствия альтернатив и относительной простоты вычисления. Обозначим $\mathcal{L}^F = \cup_{L' \in V_N^*, L'' \in V_M^*} \mathcal{L}^F(L', L'')$ и $\mathcal{D}^F = \cup_{D' \in V_N, D'' \in V_M} \mathcal{D}^F(D', D'')$. Также введем в рассмотрение множества $\mathcal{L}_0^F = \{\mathcal{L} \in \mathcal{L}^F : (l_i'' = 0) \Rightarrow (l_i' = 0), i = 1, 2, \dots, k\}$ и $\mathcal{D}_0^F = \{\mathcal{D} \in \mathcal{D}^F : (d_i'' = 0) \Rightarrow (d_i' = 0), i = 1, 2, \dots, k\}$. Принимая во внимание (4) и (6), заведомо имеем $\tilde{\delta}_{\mathcal{L}} = 0$ при $\mathcal{L} \in \mathcal{L}^F \setminus \mathcal{L}_0^F$ и $\tilde{p}_{\mathcal{D}} = 0$ при $\mathcal{D} \in \mathcal{D}^F \setminus \mathcal{D}_0^F$. Отсюда следует, что самостоятельными и практически значимыми для линейного и разностного методов являются задачи по нахождению следующих величин:

$$\tilde{\delta}^F = \max_{\mathcal{L} \in \mathcal{L}_0^F \setminus \{0\}} |\tilde{\delta}_{\mathcal{L}}| \quad \text{и} \quad \tilde{p}^F = \max_{\mathcal{D} \in \mathcal{D}_0^F \setminus \{0\}} \tilde{p}_{\mathcal{D}}. \quad (18)$$

Полученным таким способом величинам соответствуют (не обязательно однозначно определенные) «лидирующие» вероятностные соотношения $(\tilde{L}', \tilde{L}'')$ и $(\tilde{D}', \tilde{D}'')$. С учетом имеющихся недостатков оценок (9) и (12) верификация приближенных равенств $\tilde{\delta}^F \approx \delta_{\tilde{L}', \tilde{L}''}^F$ и $\tilde{p}^F \approx p_{\tilde{D}', \tilde{D}''}^F$ должна быть неотъемлемой частью исследований, для этого используются соответствующие статистические оценки $\hat{\delta}_{\tilde{L}', \tilde{L}''}$ и $\hat{p}_{\tilde{D}', \tilde{D}''}$ [4].

4. Показатели рассеивания линейной среды. Зачастую даже нахождение величин (18) представляет собой чрезвычайно сложную вычислительную задачу. Тогда переходят к задачам по нахождению наименьшего количества отличных от единиц сомножителей в произведениях (9) и (12). С этой целью для систем локальных вероятностных соотношений $\mathcal{L} \in \mathcal{L}_0^F$ и $\mathcal{D} \in \mathcal{D}_0^F$ вводят количественные характеристики

$$\theta_{\mathcal{L}} = \left| \{i \in \{1, 2, \dots, k\} : l_i'' \neq 0\} \right| \quad \text{и} \quad \theta'_{\mathcal{D}} = \left| \{i \in \{1, 2, \dots, k\} : d_i' \neq 0\} \right|. \quad (19)$$

Тогда естественным образом возникают величины

$$\theta_L^F = \min_{\mathcal{L} \in \mathcal{L}_0^F \setminus \{0\}} \theta_{\mathcal{L}} \quad \text{и} \quad \theta_D^F = \min_{\mathcal{D} \in \mathcal{D}_0^F \setminus \{0\}} \theta'_{\mathcal{D}}, \quad (20)$$

называемые соответственно *линейным и разностным показателями рассеивания линейной среды* [2]. Для введенных показателей уместно использовать распространенные термины «минимальное количество

линейно и разностно активных S-блоков». Независимость от нелинейных функциональных элементов является их несомненным достоинством. Показатели (20) предоставляют следующие полезные неравенства:

$$\tilde{\delta}^{\mathcal{F}} \leq \left(\max_{i \in \{1, 2, \dots, k\}} |\delta^{f_i}| \right)^{\theta_L^{\mathcal{F}}} \quad \text{и} \quad \tilde{p}^{\mathcal{F}} \leq \left(\max_{i \in \{1, 2, \dots, k\}} p^{f_i} \right)^{\theta_D^{\mathcal{F}}}. \quad (21)$$

5. Показатели рассеивания линейной среды AES-подобных алгоритмов шифрования. Большое количество работ посвящено нахождению оценок снизу для показателей рассеивания линейной среды алгоритма шифрования AES, см., например, [9, 10, 12, 16]. Часто для решения этой задачи используется *алгоритмический* подход. В [2] получены, а затем в [5] обобщены точные *теоретические* оценки для этих показателей в случае произвольного числа итераций XSLP-схемы, соответствующей широкому классу AES-подобных алгоритмов шифрования. Все упомянутые выше оценки базируются на рассеивающих характеристиках локальных матриц. Пусть $[x] \in \mathbb{N}_0$ — количество ненулевых m -векторов в mk -векторе x . Напомним (см. [2, 10]), что линейным и разностным *коэффициентами рассеивания* матрицы $B \in \text{GL}(mk, 2)$ называются соответственно величины

$$\rho_L^B = \min_{L'' \in V_{mk}^* \setminus \{0\}} ([B \cdot L''] + [L'']) \quad \text{и} \quad \rho_D^B = \min_{D' \in V_{mk} \setminus \{0\}} ([D'] + [D' \cdot B]). \quad (22)$$

Рассмотрим отображение $\text{XSLP} : V_n \rightarrow V_n$, реализующее r итераций XSLP-схемы с размером блока $n = mk^2$, $r, m, k \in \mathbb{N}$. Функциональная схема отображения $\text{XSLP} : V_n \rightarrow V_n$ определяется естественным образом (как в примере 1) и обозначается так же: XSLP. Пусть подстановки P_i являются равномерно рассеивающими, а локальные матрицы B_{i,j_1} имеют фиксированные линейный и разностный коэффициенты рассеивания ρ_L и ρ_D соответственно, $i = 1, 2, \dots, r$, $j_1 = 0, 1, \dots, k - 1$. В [5] показано, что имеют место неравенства

$$\theta_L^{\text{XSLP}} \geq S_{\min}(\rho_L, r) \quad \text{и} \quad \theta_D^{\text{XSLP}} \geq S_{\min}(\rho_D, r), \quad (23)$$

где

$$S_{\min}(\rho, r) = \begin{cases} 1, & \text{если } r = 1, \\ \rho, & \text{если } r = 2, \\ 2\rho - 1, & \text{если } r = 3, \\ \rho^2, & \text{если } r = 4, \\ S_{\min}(\rho, r - 4) + \rho^2, & \text{если } r > 4. \end{cases} \quad (24)$$

Таким образом, в рассматриваемом случае определение показателей рассеивания линейной среды сводится к вычислению соответствующих коэффициентов рассеивания локальных матриц. Несмотря на множество аргументов, оправдывающих использование локальных преобразований с максимальными коэффициентами рассеивания $\rho = k + 1$, существуют AES-подобные алгоритмы шифрования, не обладающие данным свойством, например Crypton [14], Midori [7]. Подобные примеры подчеркивают значимость общей формулы (24).

6. Коэффициенты рассеивания отображений общего вида, оценки для них и внешние показатели рассеивания линейной среды. Из определений коэффициентов рассеивания матриц (22) видно, что они равны наименьшему возможному суммарному весу нетривиальных глобальных вероятностных соотношений, которые можно построить для соответствующего линейного преобразования. Эти характеристики важны при анализе размножения ненулевых локальных вероятностных соотношений в функциональных схемах шифрпреобразований, что иллюстрируют, например, неравенства (23). Для нелинейных отображений аналогичные характеристики также представляют несомненный интерес. Пусть $G : V_{mk} \rightarrow V_{mk}$ — отображение общего вида, рассмотрим для него коэффициенты рассеивания, определенные в работе [10]:

$$\rho_L^G = \min_{\substack{L' \in V_{mk}^*, L'' \in V_{mk}^* \setminus \{0\}: \\ \delta_{L', L''}^G \neq 0}} ([L'] + [L'']) \quad \text{и} \quad \rho_D^G = \min_{\substack{D' \in V_{mk} \setminus \{0\}, D'' \in V_{mk}: \\ p_{D', D''}^G > 0}} ([D'] + [D'']). \quad (25)$$

Данные коэффициенты рассеивания являются прямым обобщением определений (22). Однако, как и соответствующие точные значения преобладания и вероятности (7), в общем случае они не поддаются вычислению даже для не слишком крупных узлов шифрпреобразований.

Следуя логике определения оценок для линейной и разностной характеристик, а также показателей рассеивания линейной среды, введем следующие характеристики для отображения общего вида $G : V_{mk} \rightarrow V_{mk}$, заданного с помощью функциональной схемы $\mathcal{G}$.

Определение 1. Оценками для линейных и разностных коэффициентов рассеивания будем называть соответственно величины

$$\tilde{\rho}_L^{\mathcal{G}} = \min_{\substack{\mathfrak{L} \in \mathcal{L}_0^{\mathcal{G}} \setminus \{0\}: \\ \tilde{\delta}_{\mathfrak{L}} \neq 0}} ([L'_{\mathfrak{L}}] + [L''_{\mathfrak{L}}]) \quad \text{и} \quad \tilde{\rho}_D^{\mathcal{G}} = \min_{\substack{\mathfrak{D} \in \mathcal{D}_0^{\mathcal{G}} \setminus \{0\}: \\ \tilde{p}_{\mathfrak{D}} > 0}} ([D'_{\mathfrak{D}}] + [D''_{\mathfrak{D}}]). \quad (26)$$

Определение 2. Внешним линейным и разностным показателями рассеивания линейной среды будем называть соответственно величины

$$\bar{\rho}_L^G = \min_{\mathfrak{L} \in \mathcal{L}_0^G \setminus \{0\}} ([L'_\mathfrak{L}] + [L''_\mathfrak{L}]) \quad \text{и} \quad \bar{\rho}_D^G = \min_{\mathfrak{D} \in \mathcal{D}_0^G \setminus \{0\}} ([D'_\mathfrak{D}] + [D''_\mathfrak{D}]). \quad (27)$$

Введенные таким образом характеристики оказываются полезными, когда в целях упрощения сложно устроенной линейной среды приходится переходить к укрупненным функциональным элементам. Они могут вычисляться с помощью локального линейного и разностного методов, наследуя их достоинства и недостатки.

7. Метод вычисления коэффициентов рассеивания линейных преобразований. Для произвольного преобразования $B \in \text{GL}(mk, 2)$ условия согласованности (10) и (11) принимают вид

$$B \cdot L'' = L' \quad \text{и} \quad D' \cdot B = D'', \quad (28)$$

где

$$L'' = \begin{pmatrix} l_1 \\ \vdots \\ l_k \end{pmatrix} \in V_{mk}^*, \quad L' = \begin{pmatrix} l_{k+1} \\ \vdots \\ l_{2k} \end{pmatrix} \in V_{mk}^*, \quad l_j \in V_m^*, \quad (29)$$

$$D' = (d_1, \dots, d_k) \in V_{mk}, \quad D'' = (d_{k+1}, \dots, d_{2k}) \in V_{mk}, \quad d_j \in V_m, \quad (30)$$

$j = 1, 2, \dots, 2k$.

Для матрицы B размеров $mk \times mk$ над полем $\text{GF}(2)$ и набора индексов $1 \leq j_1 < j_2 < \dots < j_t \leq 2k$, $2 \leq t \leq k+1$, определим матрицу $W_{j_1, \dots, j_t}^B$ размеров $(3k-t)m \times 2mk$ над полем $\text{GF}(2)$ по правилу:

$$W_{j_1, j_2, \dots, j_t}^B = \begin{pmatrix} B, I_{mk} \\ T_{i_1} \\ T_{i_2} \\ \vdots \\ T_{i_{2k-t}} \end{pmatrix}, \quad (31)$$

где $\{i_1, i_2, \dots, i_{2k-t}\} = \{1, 2, \dots, 2k\} \setminus \{j_1, j_2, \dots, j_t\}$, матрица T_i , $i = 1, 2, \dots, 2k$, размеров $m \times 2mk$ над полем $\text{GF}(2)$ определяется как

$$T_i = (O_m \dots, O_m^{i-1}, I_m^i, O_m^{i+1}, \dots, O_m^{2k}), \quad (32)$$

O_m и I_m — соответственно нулевая и единичная квадратные матрицы размеров $m \times m$ над полем $\text{GF}(2)$, $m \in \mathbb{N}$.

Теорема 3. *Справедливы следующие утверждения:*

- 1) Ненулевое согласованное линейное соотношение для преобразования $B \in \text{GL}(mk, 2)$, задаваемое вектор-столбцами $L', L'' \in V_{mk}^*$ вида (29), имеет не более $t \in \mathbb{N}$, $2 \leq t \leq k + 1$, ненулевых t -векторов $l_j \in V_m^* \setminus \{0\}$, с индексами $j \in \{j_1, j_2, \dots, j_t\}$, $1 \leq j_1 < j_2 < \dots < j_t \leq 2k$, тогда и только тогда, когда $\text{rank } W_{j_1, j_2, \dots, j_t}^B < 2mk$.
- 2) Ненулевое согласованное разностное соотношение для преобразования $B \in \text{GL}(mk, 2)$, задаваемое вектор-строками $D', D'' \in V_{mk}$ вида (30), имеет не более $t \in \mathbb{N}$, $2 \leq t \leq k + 1$, ненулевых t -векторов $d_j \in V_m \setminus \{0\}$, с индексами $j \in \{j_1, j_2, \dots, j_t\}$, $1 \leq j_1 < j_2 < \dots < j_t \leq 2k$, тогда и только тогда, когда $\text{rank } W_{j_1, j_2, \dots, j_t}^{B^\top} < 2mk$, где $B^\top$ — транспонированная матрица B .

Доказательство. Перепишем условия (28) в эквивалентном виде:

$$(B, I_{mk}) \cdot \begin{pmatrix} L'' \\ L' \end{pmatrix} = 0^\downarrow \quad \text{и} \quad (B^\top, I_{mk}) \cdot \begin{pmatrix} (D')^\top \\ (D'')^\top \end{pmatrix} = 0^\downarrow. \quad (33)$$

Используя введенные выше обозначения, выпишем в матричном виде необходимые и достаточные условия того, что t -векторы $l_i \in V_m^*$ и $d_i \in V_m$ с индексами $i \in \{i_1, i_2, \dots, i_{2k-t}\} = \{1, 2, \dots, 2k\} \setminus \{j_1, j_2, \dots, j_t\}$ являются нулевыми:

$$\begin{pmatrix} T_{i_1} \\ \vdots \\ T_{i_{2k-t}} \end{pmatrix} \cdot \begin{pmatrix} L'' \\ L' \end{pmatrix} = 0^\downarrow \quad \text{и} \quad \begin{pmatrix} T_{i_1} \\ \vdots \\ T_{i_{2k-t}} \end{pmatrix} \cdot \begin{pmatrix} (D')^\top \\ (D'')^\top \end{pmatrix} = 0^\downarrow. \quad (34)$$

Равенства (33) и (34) можно рассматривать как системы однородных линейных булевых уравнений относительно $2mk$ переменных $((L'')^\top, (L')^\top)$ и (D', D'') соответственно.

С одной стороны, ненулевое линейное (или разностное) соотношение, являющееся решением объединения соответствующих систем (33) и (34), удовлетворяет одновременно условию согласованности и ограничению на состав ненулевых t -векторов из формулировки теоремы. С другой стороны, подобное решение существует тогда и только тогда, когда матрица системы однородных линейных уравнений, совпадающая в данном случае с $W_{j_1, j_2, \dots, j_t}^B$ (или $W_{j_1, j_2, \dots, j_t}^{B^\top}$), имеет неполный ранг. Теорема доказана. $\square$

Используя критерии из теоремы 3, вычисление линейного ρ_L^B и разностного ρ_D^B коэффициентов рассеивания произвольного преобразования $B \in \text{GL}(mk, 2)$ можно проводить с помощью следующего алгоритма.

Алгоритм 1.

Вход: $B \in \text{GL}(mk, 2)$;

Выход: коэффициент рассеивания ρ_L^B (или ρ_D^B);

- 1: для всех $t = 2, 3, \dots, k$
- 2: для всех $j_1, j_2, \dots, j_t : 1 \leq j_1 < \dots < j_t \leq 2k, j_1 < k + 1, j_t > k$
- 3: если $\text{rank } W_{j_1, j_2, \dots, j_t}^B < 2mk$ (или $\text{rank } W_{j_1, j_2, \dots, j_t}^{B^\top} < 2mk$), то
- 4: подать на выход t ;
- 5: подать на выход $k + 1$;

Теорема 4. Алгоритм 1 корректен и имеет трудоемкость менее $(3mk)^2 \cdot 2^{2k}$ побитовых сложений $2mk$ -векторов по модулю 2.

Доказательство. Диапазон опробования числа t указан с учетом хорошо известных границ для коэффициентов рассеивания:

$$2 \leq \rho_L^B \leq k + 1 \text{ и } 2 \leq \rho_D^B \leq k + 1. \quad (35)$$

Индексы $j_1, j_2, \dots, j_t$ пробегают сочетания из $2k$ элементов по t . Поскольку преобразование B обратимо, то из перебора заведомо исключаются индексы, для которых $j_t \leq k$ или $j_1 \geq k + 1$. В случае если алгоритм перешел от значения $t - 1$ к t , то коэффициент рассеивания строго больше $t - 1$, так как тогда все соотношения гарантированно имеют более $t - 1$ ненулевых m -векторов. Поэтому если алгоритм подает на выход ответ при некотором $t \leq k$, то это означает, что существует соотношение, в котором ровно t ненулевых m -векторов. Это число является минимально возможным, а значит, равно коэффициенту рассеивания.

При фиксированном $t = 2, 3, \dots, k$ количество перебираемых индексов равно $\binom{2k}{t} - 2\binom{k}{t}$, где $\binom{m}{n}$ — число сочетаний из m элементов по n . Тогда количество шагов перебора не превосходит $\sum_{t=2}^k (\binom{2k}{t} - 2\binom{k}{t}) < 2^{2k}$. Если применять метод Гаусса, то наибольшая трудоемкость нахождения ранга матрицы вида (31) достигается при максимальном количестве ее строк, которое строго меньше $3mk$. Метод Гаусса имеет квадратичную трудоемкость относительно элементарных операций со строками. Теорема доказана. $\square$

Замечание 1. Операции со строками выбраны в качестве элементарных для оценки трудоемкости из практических соображений, так как

широко применяются в реализациях метода Гаусса для поля $\text{GF}(2)$ и близки к арифметическим операциям с целыми числами при величине mk порядка разрядности вычислительной системы.

Замечание 2. Простая модификация алгоритма 1 позволяет также находить для заданного преобразования $B \in \text{GL}(mk, 2)$ все наборы индексов, соответствующие некоторым *выполнимым* минимальным согласованным соотношениям.

Замечание 3. Если алгоритм безуспешно перешел от значения $t - 1$ к t и был остановлен по причине больших временных затрат, то результатом является оценка снизу $\rho_L^B \geq t$ (или $\rho_D^B \geq t$).

8. Уточнение оценок для показателей рассеивания линейной среды AES-подобных алгоритмов шифрования. Формула (24) получена в предположении, что для локальных $mk \times mk$ -матриц с коэффициентом рассеивания ρ имеют место все допустимые $\binom{2k}{\rho} - 2\binom{k}{\rho}$ соотношения веса ρ . На самом деле это не всегда так.

Пример 2. Рассмотрим матрицу $B' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \in \text{GL}(mk, 2)$ при $m = 3, k = 2$. Легко убедиться, что $\rho_L^{B'} = \rho_D^{B'} = 2$. Кроме того, ненулевые линейные соотношения веса 2 для матрицы B' имеют вид $((L'_0, 0), (0, L''_1)) \in V_6^* \times V_6^*, L'_0, L''_1 \in V_3 \setminus \{0\}$. Схематически этот факт представлен на рис. 2.

Рис. 2. Допустимые линейные соотношения для матрицы из примера 2

Таким образом, оценки (23), оставаясь верными, при некоторых параметрах XSLP-схемы могут оказаться консервативными. Для того чтобы выяснить, так ли это, воспользуемся результатами из [6], где дано конструктивное описание усеченных представлений всех согласованных систем локальных линейных и разностных вероятностных соотношений с минимальным количеством активных S-блоков для XSLP-схем с равномерно рассеивающими перестановками и локальными матрицами с фиксированным коэффициентом рассеивания. Под усеченным

представлением системы при этом понимается упорядоченный набор индикаторов того, что соответствующие векторы из локальных вероятностных соотношений не равны нулю. Тогда для каждой системы можно установить, какие m -векторы из соотношения для каждой локальной матрицы являются ненулевыми. С другой стороны, теорема 3 позволяет проверить, возможно ли для данной матрицы соотношение с таким набором ненулевых m -векторов. Если соотношение не допустимо, то таковой является и система в целом.

Пример 2 (продолжение). Рассмотрим $r = 3$ итерации XSLP-схемы с размером блока $n = mk^2$ при $k = 2$. Пусть локальные матрицы равны B' , а перестановки положим равномерно рассеивающими. С помощью результатов работы [6] легко получить усеченные представления всех 16 минимальных согласованных систем локальных линейных вероятностных соотношений с точностью до выходного вектора из соотношений для матриц последней итерации (см. рис. 3).

Рис. 3. Усеченные представления всех минимальных согласованных систем локальных вероятностных соотношений для XSLP-схемы при $k = 2$ и $\rho = 2$

Нетрудно видеть, что ни одна из возможных минимальных систем не может быть реализована с учетом свойств матрицы B' . Следовательно, для рассматриваемой XSLP-схемы показатель рассеивания линейной среды строго больше $S_{\min}(2, 3) = 3$.

С другой стороны, например, в матрице $B'' = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$ с линейным коэффициентом рассеивания $\rho_L^{B''} = 2$ допустимы все линейные соотношения веса 2, что делает актуальной каждую из минимальных систем для рассматриваемой XSLP-схемы.

Теперь становится ясным алгоритм, позволяющий проверить достижимость нижних оценок (23), формулируемый одинаково для линейного и разностного показателей рассеивания.

Алгоритм 2.

Вход: параметры исследуемой XSLP-схемы;

Выход: если оценки (23) достижимы, то 1, иначе — 0;

- 1: **для всех** усеченных минимальных согласованных систем локальных вероятностных соотношений
- 2: положить $I \leftarrow 1$; // индикатор допустимости системы
- 3: **для всех** матриц B_{i,j_1} в системе
- 4: положить $I_{B_{i,j_1}} \leftarrow 0$; // индикатор допустимости матрицы
- 5: **для всех** допустимых усеченных соотношений для B_{i,j_1}
- 6: **если** соотношение для B_{i,j_1} согласуется с системой, **то**
- 7: положить $I_{B_{i,j_1}} \leftarrow 1$ и прервать цикл по соотношениям;
- 8: **если** $I_{B_{i,j_1}} = 0$, **то**
- 9: положить $I \leftarrow 0$ и прервать цикл по матрицам;
- 10: **если** $I = 1$, **то**
- 11: подать на выход 1; // допустимая система найдена
- 12: подать на выход 0; // ни одна система не оказалась допустимой

9. Применение линейного метода к AES-подобному алгоритму шифрования с учебными параметрами. Возвращаясь к общей проблеме применения линейного и разностного методов, проиллюстрируем на примере AES-подобных алгоритмов шифрования нередкую ситуацию, когда общепринятые теоретические оценки свойств шифрпреобразований расходятся с истинными значениями.

Пример 3. Рассмотрим $r = 3$ итерации XSLP-схемы с размером блока $n = mk^2$ при $m = 3$ и $k = 2$, $XSLP : V_{12} \rightarrow V_{12}$. Пусть итерационные ключи нулевые, локальные подстановки равны $\pi = (\pi(x) | x \in V_3) = \begin{pmatrix} 000 & 001 & 010 & 011 & 100 & 101 & 110 & 111 \\ 110 & 101 & 010 & 111 & 000 & 001 & 111 & 100 \end{pmatrix}$. Используя значения из примера 1, положим локальные матрицы равными B , а перестановки — P_1 . Преобразования линейных вероятностных соотношений для подстановки π представлены в табл. 1, откуда, в частности, $\delta^\pi = \frac{1}{2}$.

Для нахождения минимальных согласованных систем локальных линейных вероятностных соотношений воспользуемся перечислением их усеченных представлений (см. рис. 4). При этом имеем $\theta_L^{XSLP} = 5$.

Путем направленного перебора по всем минимальным согласованным системам можно найти такие, для которых мо-

Таблица 1. Преобразования $\delta_{l',l''}^\pi$ линейных вероятностных соотношений для подстановки π

$l' \backslash l''$	000	001	010	011	100	101	110	111
000	1	0	0	0	0	0	0	0
001	0	1/2	-1/2	0	1/2	0	0	1/2
010	0	0	1/2	-1/2	0	0	1/2	1/2
011	0	1/2	0	1/2	-1/2	0	1/2	0
100	0	0	-1/2	-1/2	-1/2	1/2	0	0
101	0	1/2	0	-1/2	0	-1/2	0	-1/2
110	0	0	0	0	-1/2	-1/2	-1/2	1/2
111	0	-1/2	-1/2	0	0	-1/2	1/2	0

Рис. 4. Усеченные представления всех минимальных согласованных систем локальных вероятностных соотношений для XSLP-схемы при $k = 2$ и $\rho = 3$

дуль оценки преобразования максимален, т.е. достигает величины $(\delta^\pi)_{\theta_L^{\text{XSLP}}} = \left(\frac{1}{2}\right)^5 = 0.003125$. Две такие системы $\mathfrak{L}_1$ и $\mathfrak{L}_2$ представлены на рис. 5.

Глобальные соотношения, определяемые по системам $\mathfrak{L}_1$ и $\mathfrak{L}_2$, задаются соответствующими вектор-столбцами: $\tilde{L}'_1 = (1, 0, 1, 0, 1, 0, 0, 0, 0, 0, 0)^\top \in V_{12}^*$ и $\tilde{L}''_1 = (1, 1, 1, 0, 1, 0, 0, 1, 1, 1, 1)^\top \in V_{12}^*$, $\tilde{L}'_2 = (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0)^\top \in V_{12}^*$ и $\tilde{L}''_2 = (1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0)^\top \in V_{12}^*$. Небольшие параметры размерности XSLP-схемы позволяют вычислять точные истинные значения преобразований любых соотношений. Первая система $\mathfrak{L}_1$ строилась таким образом, чтобы доставлять минимум модуля истинного преобразования по всем минимальным системам, а вторая $\mathfrak{L}_2$ — максимум. В итоге имеем существенно различающиеся значения $\delta_{\tilde{L}'_1, \tilde{L}'_1}^{\text{XSLP}} = 0$ и $\delta_{\tilde{L}'_2, \tilde{L}'_2}^{\text{XSLP}} = -\frac{111}{512} = -0.216796875$. Вместе с тем оба значения далеки как от своих теоретических оценок

Рис. 5. Две минимальные системы согласованных локальных линейных вероятностных соотношений для XSLP-схемы из примера 3

$|\tilde{\delta}_{\mathcal{L}_1}| = |\tilde{\delta}_{\mathcal{L}_2}| = 0.003125$, так и от истинной линейной характеристики $\delta^{\text{XSLP}} = 0.75$, которая достигается, например, при вектор-столбцах $L'_{\max} = (0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0)^{\top} \in V_{12}^*$, $L''_{\max} = (0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0)^{\top} \in V_{12}^*$, при этом $\delta_{L'_{\max}, L''_{\max}}^{\text{XSLP}} = -0.75$.

Можно допустить, что отличие линейной характеристики от ее оценок уменьшается с ростом размерности шифрпреобразования. Вместе с тем любые подобные предположения все еще очень далеки от строгих обоснований. Например, с большой осторожностью следует принимать так называемую *гипотезу о стохастической эквивалентности ключей* [13, с. 148], анализируя вместо этого шифрпреобразования при как можно большем количестве ключей.

В заключение автор выражает благодарность Ф.М. Малышеву за ценные замечания, полезное обсуждение теоретических аспектов линейного и разностного методов и в особенности за проверку упрощенных доказательств принадлежащих ему теорем 1 и 2.

Список литературы

- [1] Малышев Ф.М., “Двойственность разностного и линейного методов в криптографии”, *Математические вопросы криптографии*, **5:3** (2014), 35–47.
- [2] Малышев Ф.М., Трифионов Д.И., “Рассеивающие свойства XSLP-шифров”, *Математические вопросы криптографии*, **7:3** (2016), 47–60.
- [3] Ерохин А.В., Малышев Ф.М., Тришин А.Е., “Многомерный линейный метод и показатели рассеивания линейной среды шифрпреобразований”, *Математические вопросы криптографии*, **8:4** (2017), 29–62.
- [4] Малышев Ф.М., Тришин А.Е., “Линейный и разностный методы в криптографии (другой взгляд)”, *Алгебра, теория чисел и дискретная геометрия: современные проблемы и приложения. Материалы XV междунар. конф., посвящ. столетию со дня рождения Н.М. Коробова, Тула, 2018*, 42–45.
- [5] Федченко В.А., “Показатели рассеивания линейной среды AES-подобных алгоритмов шифрования”, *Математические вопросы криптографии*, **8:3** (2017), 109–126.
- [6] Федченко В.А., “Минимальные согласованные системы локальных вероятностных соотношений в AES-подобных алгоритмах шифрования”, *Математические вопросы криптографии*, **9:3** (2018), 127–142.
- [7] Banik S., Bogdanov A., Isobe T., Shibuta K., Hiwatari H., Akishita T., Regazzoni F., “Midori: A Block Cipher for Low Energy”, *Advances in Cryptology — ASIACRYPT’2015*, *Lect. Notes Comput. Sci.*, **9453**, 2015, 411–436.
- [8] Biham E., Shamir A., “Differential cryptanalysis of DES-like cryptosystems”, *Lect. Notes Comput. Sci.*, **537**, 1991, 2–21.
- [9] Biryukov A., Nikolic I., “Automatic search for related-key differential characteristics in byte-oriented block ciphers: applications to AES, Camellia, Khazad and Others”, *EUROCRYPT’2010*, *Lect. Notes Comput. Sci.*, **6110**, 2010, 322–344.
- [10] Daemen J., Rijmen V., *The Design of Rijndael: AES — The Advanced Encryption Standard*, Heidelberg etc. : Springer, 2002, 238 pp.
- [11] Daemen J., Govaerts R., Vandewalle J., “Correlation matrices”, *Lect. Notes Comput. Sci.*, **1008**, 1995, 275–285.
- [12] Fouque P.-A., Jean J., Peyrin T., “Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128”, *CRYPTO’2013*, *Lect. Notes Comput. Sci.*, **8042**, 2013, 183–203.
- [13] Knudsen L.R., Robshaw M.J.B., *The Block Cipher Companion*, Springer, 2011, 267 c.
- [14] Lim C.H., “A revised version of Crypton: Crypton v1.0”, *FSE 1999*, *Lect. Notes Comput. Sci.*, **1636**, 1999, 31–45.
- [15] Matsui M., “Linear cryptanalysis method for DES cipher”, *Lect. Notes Comput. Sci.*, **765**, 1994, 386–397.
- [16] Mouha N., Wang Q., Gu D., Preneel B., “Differential and linear cryptanalysis using mixed-integer linear programming”, *INSCRYPT’2011*, *Lect. Notes Comput. Sci.*, **7537**, 2012, 57–76.
- [17] Nyberg K., “Linear approximation of block ciphers”, *EUROCRYPT’1994*, *Lect. Notes Comput. Sci.*, **950**, 1994, 439–444.