Math-Net.Ru

Общероссийский математический портал

Ф. М. Малышев, Д. И. Трифонов, Рассеивающие свойства XSLP-шифров, *Матем. вopr. криптогр.*, 2016, том 7, выпуск 3, 47–60

DOI: <https://doi.org/10.4213/mvk195>

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: 54.164.48.24

26 апреля 2023 г., 02:16:20

Рассеивающие свойства XSLP-шифров

Ф. М. Малышев¹, Д. И. Трифонов²

¹ Математический институт им. В. А. Стеклова Российской академии наук, Москва

² Технический комитет по стандартизации (ТК 26), Москва

Получено 20.IV.2015

Аннотация. Получена точная нижняя оценка числа локальных подстановок в XSLP-шифре с произвольным числом итераций, по сумме вероятностных линейных соотношений которых строится вероятностное линейное соотношение между знаками открытого и зашифрованного текстов. В исследуемом шифре матрицы L линейных преобразований являются блочно-диагональными с максимально рассеивающими блоками, а коммутации P — равномерно рассеивающими.

Ключевые слова: линейный криптоанализ, шифрпреобразование, XSL-шифры, SP-сети, XSLP-схемы, XSPL-схемы

Diffusion properties of XSLP-ciphers

F. M. Malyshev¹, D. I. Trifonov²

¹ Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

² Technical committee for standardization (TC26), Moscow

Abstract. We obtain an exact lower estimate for the number of local permutations in XSLP-cipher with an arbitrary number of rounds. The sum of linear probabilistic relations of these permutations forms the linear probabilistic relation connecting the bits of the plain text and that of the cipher text. In the considered ciphers the matrices L of linear transformations are block-diagonal with maximally diffusive blocks and permutations P are uniformly diffusive.

Key words: linear cryptanalysis, encryption transformation, XSL-ciphers, SP-networks, XSLP-scheme, XSPL-scheme

Citation: *Mathematical Aspects of Cryptography*, 2016, v. 7, № 3, pp. 47–60 (Russian)

© Академия криптографии Российской Федерации, 2016 г.

1. XSLP-шифры

Рассматриваемые в статье шифры, реализуемые XSLP-схемами, преобразуют за r итераций блоки открытой информации по $n = m \cdot k^2$ бит в блоки шифрованной информации той же длины. Основными параметрами этих шифров на i -й итерации, $i = 1, 2, \dots, r$, являются:

1) локальные подстановки $\pi_{ij} \in S_{V_m}$, $\pi_{ij}: V_m \rightarrow V_m$, $V_m \stackrel{\text{def}}{=} GF(2)^m$, $j = 0, 1, \dots, k^2 - 1$, независимо действующие на k^2 не пересекающихся подблоках длины m бит, называемых в статье m -векторами,

2) невырожденные матрицы $B_{ij_1} \in GL(mk, 2)$, $j_1 = 0, 1, \dots, k - 1$, независимо действующие умножением справа на mk -векторы, состоящие из k выписанных подряд m -векторов,

3) подстановка $P_i: \{0, 1, \dots, k^2 - 1\} \rightarrow \{0, 1, \dots, k^2 - 1\}$, $P_i \in S_{k^2}$, реализующая перестановку всех m -векторов a_j в блоке $a = (a_0, a_1, \dots, a_{k^2-1}) \in V_n$, $a_j \in V_m$, $j = 0, 1, \dots, k^2 - 1$. Соответствующее преобразование V_n обозначаем $\hat{P}_i: V_n \rightarrow V_n$,

$$\hat{P}_i(a_0, a_1, \dots, a_{k^2-1}) = (a_{P_i^{-1}(0)}, a_{P_i^{-1}(1)}, \dots, a_{P_i^{-1}(k^2-1)}).$$

Из матриц $B_{ij_1} \in GL(mk, 2)$, $j_1 = 0, 1, \dots, k - 1$, составляется блочно-диагональная матрица $L_i \in GL(mk^2, 2)$, $i = 1, 2, \dots, r$.

В современных шифрах такого типа чаще всего $m = 8$.

Для номеров m -векторов $j = 0, 1, \dots, k^2 - 1$ будем пользоваться k -ичной записью в виде пары «цифр»: $j = (j_0, j_1) = j_0 + j_1 \cdot k$, $j_0, j_1 \in \{0, 1, \dots, k - 1\}$. При такой записи j_0 — номер m -вектора в mk -векторе с номером j_1 ; mk -вектор с номером $j_1 \in \{0, 1, \dots, k - 1\}$ в блоке $a \in V_n$ будем обозначать a_{*j_1} : $a_{*j_1} = (a_{(0, j_1)}, a_{(1, j_1)}, \dots, a_{(k-1, j_1)})$, $a_{(j_0, j_1)} \in V_m$, $j_0 = 0, 1, \dots, k - 1$.

На i -й итерации, $i = 1, \dots, r$, с итерационным ключом $z_i \in V_n$ блок $a = (a_0, a_1, \dots, a_{k^2-1})$ преобразуется в блок $b = (b_0, b_1, \dots, b_{k^2-1})$, $a_j, b_j \in V_m$, $j = 0, 1, \dots, k^2 - 1$, посредством четырех подробно определяемых ниже операций, реализующих подстановки на V_n :

$$a \xrightarrow{X_i} u \xrightarrow{S_i} v \xrightarrow{L_i} w \xrightarrow{\hat{P}_i} b. \quad (1)$$

В результате применения операций $X_i, S_i, L_i, \hat{P}_i$ получаем промежуточные блоки $u, v, w \in V_n$, при этом:

$$\begin{aligned} u &= a + z_i = T_{z_i}(a) \text{ — сдвиг } a \text{ на ключевой вектор } z_i, \quad X_i = T_{z_i}; \\ v &= S_i(u), \quad S_i = (\pi_{i0}, \pi_{i1}, \dots, \pi_{i, k^2-1}), \quad v_j = \pi_{ij}(u_j), \quad j = 0, 1, \dots, k^2 - 1; \\ w &= v \cdot L_i, \quad w_{*j_1} = v_{*j_1} \cdot B_{ij_1}, \quad j_1 = 0, 1, \dots, k - 1; \\ b &= \hat{P}_i(w), \quad b_j = w_{P_i^{-1}(j)}, \quad j = 0, 1, \dots, k^2 - 1. \end{aligned}$$

При любой из $24 = 4!$ перестановок операторов в (1) будем получать свои схемы реализации XSLP-шифра. Это легко понять, учитывая равенства

$$T_z L_i = L_i T_{z L_i}, \quad T_z \hat{P}_i = \hat{P}_i T_{\hat{P}_i(z)}, \quad z \in V_n,$$

$$S_i \hat{P}_i = \hat{P}_i \tilde{S}_i, \quad \tilde{S}_i = (\tilde{\pi}_{i0}, \tilde{\pi}_{i1}, \dots, \tilde{\pi}_{i,k^2-1}) = (\pi_{i,P_i^{-1}(0)}, \pi_{i,P_i^{-1}(1)}, \dots, \pi_{i,P_i^{-1}(k^2-1)}),$$

$$\tilde{\pi}_{ij} = \pi_{i,P_i^{-1}(j)}, \quad j = 0, 1, \dots, k^2 - 1.$$

Здесь и далее подстановки в произведениях применяются в порядке слева направо.

Если требуется подчеркнуть конкретную реализацию шифра, то вместо термина «шифр» правильной использовать термин «схема». Тогда при обозначении XSLP-шифра используем термин «XSLP-схема» как основной, но допустимы и все остальные 23 возможные схемы, вплоть до PLSX-схемы.

Например, в описаниях алгоритма шифрования AES (см. [1–3]), относящегося к XSLP-шифрам, операторы $L_i, \hat{P}_i$ в цепочке (1) следуют в другом порядке. Для шифров типа AES имеем:

$$\begin{aligned} \prod_{i=1}^r (T_{z_i} S_i \hat{P}_i L_i) &= \prod_{i=1}^r (T_{z_i} \hat{P}_i \tilde{S}_i L_i) = \prod_{i=1}^r (\hat{P}_i T_{\hat{P}_i(z_i)} \tilde{S}_i L_i) = \\ &= \hat{P}_1 \cdot \prod_{i=1}^r (T_{\hat{P}_i(z_i)} \tilde{S}_i L_i \hat{P}_{i+1}) \cdot \hat{P}_{r+1}^{-1}. \end{aligned}$$

Перестановка m -векторов $\hat{P}_{r+1}$ может быть любой, например $\hat{P}_{r+1} = \hat{P}_1$.

Из 24 возможностей именно XSLP-схема выбрана не случайно. В XSLP-схеме присутствуют обе хорошо зарекомендовавшие себя конструкции: XSL-схемы и SP-сети. Шифрпреобразования, задаваемые остальными 23 схемами (после возможного домножения их на не зависящие от криптографического ключа шифрпреобразования), сопряжены шифрпреобразованию XSLP-схемы посредством преобразований, также не зависящих от ключа. Как и в случае AES, в этом легко (и полезно) убедиться непосредственно, используя указанную выше возможность перестановки соседних операторов в парах $\{X, L\}$, $\{X, P\}$, $\{S, P\}$. (Указанная «сопряженность» не есть следствие того, что симметрическая группа на множестве $\{X, L, P, S\}$ порождается тремя последовательными транспозициями (L, X) , (X, P) , (P, S) . В случае пяти и более операторов подобное заключение привело бы к ложному выводу.)

Конечно, все 24 перестановки символов X, S, L, P перебирать не обязательно. Можно их разбить на 6 подмножеств по 4 перестановки, отвечающих 6 возможным ожерельям из 4 «бусинок» X, S, L, P . Два ожерелья объявим смежными, если одно из другого получается одной из трех выше указанных перестановок соседних «бусинок». Отношение смежности задает связный граф на 6 вершинах, что и служит формальным доказательством взаимной «сопряженности» шифрпреобразований 24 рассматриваемых схем.

На i -й итерации XSLP-схемы, $i = 1, 2, \dots, r$, XSL-схемами реализуются k подстановок

$$T_{z_i, *j_1} S_{i, *j_1} B_{ij_1} : V_{mk} \rightarrow V_{mk}, \quad j_1 = 0, 1, \dots, k-1.$$

Здесь $S_{i, *j_1} = (\pi_{i, (0, j_1)}, \pi_{i, (1, j_1)}, \dots, \pi_{i, (k-1, j_1)})$, а $z_{i, *j_1}$ — mk -вектор в z_i с номером j_1 . Данные XSL-схемы (при основном алфавите $A = GF(2)$) за одну итерацию при каждом $j_1 = 0, 1, \dots, k-1$ осуществляют биекции $A^{mk} \rightarrow A^{mk}$ с помощью наложения ключа, локальных подстановок $\pi_{i, (j_0, j_1)} \in S_{A^m}$, $j_0 = 0, 1, \dots, k-1$, и матрицы $B_{ij_1} \in GL(mk, A)$.

Все r итераций XSLP-схемы можно рассматривать как SP-сеть, на i -й итерации которой, $i = 1, 2, \dots, r$, реализуется биекция $\bar{A}^{k \cdot k} \rightarrow \bar{A}^{k \cdot k}$, $\bar{A} \stackrel{\text{def}}{=} V_m$, с помощью локальных подстановок $T_{z_i, *j_1} S_{i, *j_1} B_{ij_1} \in S_{\bar{A}^k}$, $j_1 = 0, 1, \dots, k-1$, и перестановки $\hat{P}_i$. Буквами основного алфавита $\bar{A} = A^m = V_m$ являются уже не биты, а m -векторы.

По большому счету, SP-сеть тоже является XSL-схемой, но матрицы в ней являются подстановочными — относятся к очень частному виду. Собственно, и XSLP-схема является XSL-схемой, в которой матрица тоже относится к частному виду — является произведением блочно-диагональной и подстановочной матриц. Но в структуру далее рассматриваемых XSL-схем такого вида с не лучшими матрицами закладываются и старый принцип построения блочных шифров в виде SP-сетей с наилучшими коммутациями, и новый принцип в виде XSL-схем с наилучшими матрицами.

При выборе блоков B_{ij_1} в матрицах L_i и подстановок P_i для конкретных шифров полезно учитывать требование рассеивания к шифрам, сформулированное К. Шенноном в связи с повышением их практической стойкости.

Необходимость в представленной структуре XSLP-шифра объясняется в следующем параграфе как компромисс между стойкостью относительно линейного метода криптографического анализа и высокими эксплуатационными характеристиками соответствующих шифраторов.

2. Эволюция требований Шеннона к блочным шифрам

В своей работе [4] на с. 394–399 Шеннон на качественном уровне сформулировал два требования к шифрам для обеспечения их высокой практической стойкости. Это «рассеивание» и «перемешивание» (в оригинале «diffusion» и «confusion»). К 60-м годам XX века эти рекомендации утвердились в появившихся тогда SP-сетях (см. [5,6]), в которых чередуются преобразования с высоким локальным перемешиванием (S -боксы), но со слабым рассеиванием, и преобразования, напротив, с высоким рассеиванием (глобальные перестановки бит), но без признаков перемешивания. В том или ином виде принцип SP-сетей присутствует в шифраторах LUCIFER [7], DES, ГОСТ 28147-89 [8]. В идейном плане принцип SP-сетей восходит к квадрату Полибия (III век до н. э.), названному Шенноном дробным шифром.

Первоначально степень рассеивания коммутаций в SP-сетях оценивалась качественно по характеру лавинного эффекта. Руководствуясь этим соображением, в случае SP-сети, реализующей на i -й итерации, $i = 1, 2, \dots, r$, выбирают отображение

$$S_i \hat{P}_i : V_{m^2} \rightarrow V_{m^2}, \quad (2)$$

где $S_i = (\pi_{i,0}, \pi_{i,1}, \dots, \pi_{i,m-1})$, $\pi_{i,j_1} \in S_{V_m}$, $j_1 = 0, 1, \dots, m-1$, $\hat{P}_i$ переставляет биты блока $a = (a_0, a_1, \dots, a_{m^2-1}) \in V_{m^2}$, $\hat{P}_i(a_0, a_1, \dots, a_{m^2-1}) = (a_{P_i^{-1}(0)}, a_{P_i^{-1}(1)}, \dots, a_{P_i^{-1}(m^2-1)})$, $P_i \in S_{m^2}$ — подстановка на множестве $\{0, 1, \dots, m^2-1\}$. Номер $j \in \{0, 1, \dots, m^2-1\}$ бита a_j в блоке a представляем в m -ичном виде: $j = (j_0, j_1) = j_0 + mj_1$, здесь $j_0 \in \{0, 1, \dots, m-1\}$ — младшая цифра, $j_1 \in \{0, 1, \dots, m-1\}$ — старшая. Естественно потребовать, чтобы при каждом фиксированном $j_1 \in \{0, 1, \dots, m-1\}$ среди старших цифр j'_1 в номерах $P_i(j_0, j_1) = (j'_0, j'_1)$, $j_0 = 0, 1, \dots, m-1$, встречались бы все m цифр. Другими словами, при каждом $j_1 \in \{0, 1, \dots, m-1\}$

$$\left| \left\{ \left[\frac{P_i(j_0, j_1)}{m} \right] : j_0 = 0, 1, \dots, m-1 \right\} \right| = m.$$

Благодаря такому свойству подстановки P_i на $(i+1)$ -й итерации среди m координат аргумента каждой подстановки π_{i+1,j'_1} , $j'_1 = 0, 1, \dots, m-1$, окажется один бит из результата применения (на предыдущей i -й итерации) подстановки π_{i,j_1} , причем это справедливо, опять же, для всех $j_1 = 0, 1, \dots, m-1$. Подстановки $P_i : \{0, 1, \dots, m^2-1\} \rightarrow \{0, 1, \dots, m^2-1\}$ с описанным свойством относятся к так называемым равномерно рассеивающим подстановкам, дуги в циклах которых содержатся среди дуг обобщенных графов де Брейна [9].

Оператор $X_i = T_{z_i}$ в формуле (2) не указан, для нас он не принципиален. Можно считать, что подстановка π_{ij_1} зависит от m -вектора ключа $z_{i,*j_1}$, $i = 1, 2, \dots, r$, $j_1 = 0, 1, \dots, m-1$.

Перемешивающие подстановки π_{ij_1} назовем локальными. Для подстановок $\hat{P}_i: V_{m^2} \rightarrow V_{m^2}$ лучше пользоваться синонимом и называть их перестановками (компонент вектора) или коммутациями.

Основным (в некотором смысле единственным) примером равномерно рассеивающей подстановки на множестве $\{0, 1, \dots, m^2 - 1\}$ является $\varkappa: (j_0, j_1) \mapsto (j_1, j_0)$. Любая равномерно рассеивающая подстановка P к ней сводится. Чтобы пояснить это, введем подстановки $P_f: \{0, 1, \dots, m^2 - 1\} \rightarrow \{0, 1, \dots, m^2 - 1\}$, задаваемые отображениями $f: \{0, 1, \dots, m-1\} \rightarrow S_{\{0,1,\dots,m-1\}}: P_f(j_0, j_1) = (f(j_1)[j_0], j_1)$. Для каждой равномерно рассеивающей подстановки P существуют однозначно задаваемые отображения f, g , для которых $P_f P P_g = \varkappa$. Это следует из того, что для каждой из m^2 пар $j_1, j'_1 \in \{0, 1, \dots, m-1\}$ имеются ровно один такой номер $j_0 \in \{0, 1, \dots, m-1\}$, что $P(j_0 + j_1 m) = j'_0 + j'_1 m$, $j'_0 \in \{0, 1, \dots, m-1\}$, и ровно один такой номер $\tilde{j}_0 \in \{0, 1, \dots, m-1\}$, что $\varkappa(j_0 + j_1 m) = \tilde{j}'_0 + j'_1 m$, $\tilde{j}'_0 \in \{0, 1, \dots, m-1\}$. Отображения f и g выбираются так, что $f(j_1)[\tilde{j}_0] = j_0$, $g(j'_1)[j'_0] = \tilde{j}'_0$.

Таким образом, хоть число равномерно рассеивающих подстановок и равно $m!^{2m}$ (числу возможных пар отображений (f, g)), но любая SP-сеть для $n = m^2$ с равномерно рассеивающими коммутациями имеет эквивалентное задание, в котором все коммутации совпадают с $\hat{\varkappa}: V_{m^2} \rightarrow V_{m^2}$. Точнее, имеют место равенства $\widehat{P_{g_0}}^{-1} (\prod_{i=1}^r S_i \hat{P}_i) \widehat{P_{g_r}} = \prod_{i=1}^r (\widehat{P_{g_{i-1}}}^{-1} S_i \widehat{P_{f_i}}^{-1} \cdot \widehat{P_{f_i}} \widehat{P_i} \widehat{P_{g_i}}) = \prod_{i=1}^r (\tilde{S}_i \cdot \hat{\varkappa})$, где $\tilde{S}_i = (\tilde{\pi}_{i,0}, \tilde{\pi}_{i,1}, \dots, \tilde{\pi}_{i,m-1})$, $\tilde{\pi}_{i,j_1} = \widehat{P_{g_{i-1}}}(j_1)^{-1} \cdot \widehat{P_{f_i}} \widehat{P_i} \widehat{P_{g_i}}(j_1)^{-1}$ ($i = 1, \dots, r$, $j_1 = 0, 1, \dots, m-1$), $g_0(j_1) \equiv id_{\{0,1,\dots,m-1\}}$, $f_i, g_i: \{0, \dots, m-1\} \rightarrow S_{\{0,\dots,m-1\}}$ удовлетворяют условиям $P_{f_i} P_i P_{g_i} = \varkappa$ при всех $i = 1, \dots, r$.

Переход от SP-сетей к XSL-схемам позволил повысить стойкость относительно линейного [10] и предшествовавшего ему разностного [11] методов криптографического анализа. С общих позиций эти методы описаны в [12] с учетом их двойственности, на которую было обращено внимание еще в [13]. Эти методы позволили глубже осмыслить введенное Шенноном качественное понятие рассеивания и дать способ измерения рассеивания вводимой ниже целочисленной характеристикой.

В [12] линейный метод нацелен на получение вероятностного линейного соотношения для шифрпреобразования

$$F: V_N \times V_K \rightarrow V_M, \quad V_N \times V_K \ni (a, z) \mapsto b = F(a, z) \in V_M, \quad (3)$$

общего вида, задаваемого функциональной схемой, которая представляется последовательностью выполняемых в определенном порядке линейных и нелинейных преобразований. Для блочного шифрования в (3) $M = N$, a и b — соответствующие блоки открытого и зашифрованного текстов, z — ключ. Предполагается, что биты ключа в процессе выполнения шифрпреобразования складываются по $\text{mod } 2$ с соответствующими промежуточными знаками.

Последовательность преобразований функциональной схемы можно представлять в виде списка команд компьютерной программы без циклов. Пусть нелинейные операции в этой программе

$$f_i: V_{n_i} \rightarrow V_{m_i}, x_i \mapsto y_i = f_i(x_i), i = 1, \dots, s, \quad (4)$$

следуют в указанном порядке. Значения переменных $x_i \in V_{n_i}$, $y_i \in V_{m_i}$ и $b \in V_M$ однозначно задаются значениями $a \in V_N$ и $z \in V_K$. В промежутках между операциями (4) (а также в начале и в конце программы) могут быть линейные преобразования.

Основной целью линейного метода, применительно к шифрпреобразованию (3), является нахождение трех конкретных булевых векторов-столбцов L', L и $L'' \neq 0$ размерностей, соответственно, N, K и M , для которых булева случайная величина $\eta = aL' + zL + bL''$ имеет как можно большее значение $\delta = |2\mathbf{P}\{\eta=0\} - 1|$, если случайный вектор a имеет равномерное распределение на V_N , а ключ $z \in V_K$ фиксирован.

Случайная величина η определяется по набору векторов-столбцов $\mathcal{L} = ((l'_i, l''_i), i = 1, \dots, s)$ размерностей, соответственно, n_i и m_i равенством

$$\eta = \sum_{i=1}^s \eta_i, \eta_i = x_i l'_i + y_i l''_i, i = 1, \dots, s. \quad (5)$$

Часто при построении набора $\mathcal{L}$ вместо максимизации величины δ , характеризующей η , прибегают к максимизации величины $\tilde{\delta} = \prod_{i=1}^s |\delta_i|$, $\delta_i = 2\mathbf{P}\{\eta_i=0\} - 1 (i = 1, \dots, s)$, причем последние вероятности вычисляются в предположении о равномерности распределений случайных векторов x_i на V_{n_i} . Когда биты ключа z складываются по $\text{mod } 2$ с соответствующими промежуточными знаками шифрпреобразования, ключ z может влиять только на знаки величин δ_i , а величина $\tilde{\delta}$ от z не зависит.

Чтобы такая сумма приняла вид $aL' + zL + bL''$ для каких-либо векторов-столбцов $L', L, L'' \neq 0$, набор $\mathcal{L}$ должен удовлетворять специальным условиям согласованности. Для их формулировки компоненты l'_i разместим на функциональной схеме как метки соответствующих входных компонент x_i ,

а компоненты l_i'' — как метки выходных компонент y_i . Расстановка меток (элементов $GF(2)$) распространяется и на каждую линейную операцию в шифрпреобразовании (3). При этом если задаваемая умножением на матрицу функция $g: V_n \rightarrow V_m$, $V_n \ni x \mapsto y = xg \in V_m$, есть одна из линейных операций в шифрпреобразовании (3), и метки входов g образуют вектор-столбец α' размерности n , а метки выходов g образуют вектор-столбец α'' размерности m , то для обеспечения равенства $x\alpha' = y\alpha'' = xg\alpha''$ или $x(\alpha' + g\alpha'') = 0$, условие согласованности предполагает выполнение равенства $\alpha' + g\alpha'' = 0$ или $\alpha' = g\alpha''$. В частности, метки вокруг сумматора $(x_1, \dots, x_n) \mapsto x_1 + \dots + x_n = y_1$ одинаковы, а метки вокруг узла разномножения $x \mapsto (x, \dots, x) = (y_1, \dots, y_m)$ в сумме дают нуль. При $n = m$ и $g = id_{V_n}$ обязательно $\alpha' = \alpha''$. Последнее означает, что если выход некоторого отображения (4) в шифрпреобразовании (3) является входом какого-то одного (другого) отображения (4), то этим выходу и входу приписываются одинаковые метки.

Пара (l_i', l_i'') в наборе $\mathcal{L}$, для которой $l_i' \neq 0, l_i'' = 0$ или $l_i' = 0, l_i'' \neq 0$, а f_i биективно, считается дефектной. В этих случаях при случайном равновероятном $x_i \in V_{n_i}$ слагаемое $\eta_i = x_i \cdot l_i' + y_i \cdot l_i'' = x_i \cdot l_i' + f_i(x_i) \cdot l_i''$ в (5) имеет равномерное распределение на $GF(2)$, поэтому $\delta_i = 0$ и, как следствие, $\tilde{\delta} = 0$.

Пусть W — совокупность всех согласованных наборов пар векторов-столбцов $\mathcal{L} = ((l_i', l_i''), i = 1, 2, \dots, s)$ без дефектов, в которых хотя бы один вектор-столбец ненулевой. Обозначим $\theta_{\mathcal{L}} = |\{i = 1, 2, \dots, s : l_i'' \neq 0\}|$.

Для уменьшения неопределенности суммы (5) нужно уменьшать неопределенности отдельных слагаемых. Они минимальны при $l_i' = 0, l_i'' = 0$. Поэтому становится важной характеристика

$$\theta = \min_{\mathcal{L} \in W} \theta_{\mathcal{L}} \quad (6)$$

шифрпреобразования (3), точнее, линейной среды этого шифрпреобразования, образованной всеми линейными преобразованиями соответствующей функциональной схемы. Замена совокупности нелинейных отображений любыми другими отображениями при тех же n_i, m_i никак не скажется на величине θ . Но чем больше θ , тем проще (за счет выбора нелинейных отображений (4)) добиваться необходимого уровня стойкости относительно линейного метода.

В разделе 3 статьи параметр θ будет определяться для XSLP-схем, введенных в разделе 1. Пока же обратимся к задаче (6) для XSL-схемы на $r = 2$ итерациях и с длиной блока $n = m^2$, как это было в (2).

В XSL-схеме биты ключа z складываются по $\text{mod } 2$ с промежуточными знаками шифрпреобразования. Такое наложение ключа выше предполагалось

при описании линейного метода. Это позволяет при определении показателя θ считать $z = 0$, т. е. можно ограничиваться рассмотрением SL-сетей.

При $r = 2$ шифрпреобразование (3) тогда примет вид $S_1 L_1 S_2 L_2$. Пусть $\mathcal{L}$ — ненулевой согласованный набор столбцов без дефектов и l — столбец длины m^2 , составленный из m столбцов l_{j_1} , $j_1 = 0, 1, \dots, m-1$, по m бит, которые образованы метками аргументов подстановок π_{2,j_1} . Пусть $[[l]] = |\{j_1 = 0, 1, \dots, m-1 : l_{j_1} \neq 0\}|$. Тогда $\theta_{\mathcal{L}} = [[L_1 l]] + [[l]]$ и $\theta = \min_{l \neq 0} \{[[L_1 l]] + [[l]]\}$.

Таким образом, получили характеристику матрицы $L_1 \in GL(m^2, 2)$. Обозначим ее через ρ_{L_1} . Нетрудно понять, что для SL-сети с r итерациями справедливо неравенство $2\theta \geq 1 + \rho_{L_1} + \dots + \rho_{L_{r-1}} + 1$, поэтому чем больше значения ρ_{L_i} , $i \in \{1, 2, \dots, r-1\}$, тем на большую стойкость шифра к линейному методу можно надеяться.

Показатель ρ_L аналогично определяется для матрицы $L \in GL(mk, 2)$, разбитой на k полос по m строк и на k колонок по m столбцов: $\rho_L = \min_{l \neq 0} \{[[Ll]] + [[l]]\}$. Здесь предполагается, что двоичные векторы-столбцы l размерности mk разбиваются на k подвекторов-столбцов размерности m и $[[l]]$ — число ненулевых подвекторов-столбцов в l . Непосредственно из определений следуют неравенства $2 \leq \rho_L \leq k + 1$. Для подстановочных матриц $\rho_L = 2$ — минимально возможное значение. Равенство $\rho_L = k + 1$ равносильно тому, что невырождены все подматрицы L на пересечении i полос и i колонок, $i = 1, 2, \dots, k$. Этот простой критерий, тоже непосредственно следующий из определений, формулировался также А. В. Анашкиным. По аналогии с равномерно рассеивающими коммутациями матрицу $L \in GL(mk, 2)$ с $\rho_L = k + 1$ следует считать максимально рассеивающей, а сам показатель ρ_L естественно называть в общем случае коэффициентом рассеивания матрицы L . Такие матрицы вводятся также в [14]. Показатель θ для линейной среды служит удачным параметром для оценки рассеивающих свойств шифрпреобразования (3).

В свете вышесказанного стал оправданным переход в SP-сетях от коммутаций P к более сложным для реализации невырожденным матрицам общего вида, так как они обеспечивают более высокие показатели рассеивания. На смену SP-сетям пришли XSL-схемы. После разработки линейного и разностного методов появилось осознание того, что для обеспечения высоких показателей перемешивания и рассеивания не имеет смысла выбирать матрицы и локальные подстановки зависящими от криптографического ключа. Ключ был вынесен за пределы этих операторов (и именно в виде покомпонентного наложения по mod 2) с тем, чтобы не изменять вероятностные характеристики локальных подстановок. Введение терминов «XSL-шифр» и «XSL-схема» (а не

«SL-сеть») как раз и отражает данное положение вещей. Для SP-сетей, возникших до линейного и разностного методов, не требовалось вводить специально выделяемый оператор для ключа (ключевыми могли быть как коммутации, так и локальные подстановки), поэтому и не возникал термин «XSP-сеть».

При комплексном учете стойкости и эксплуатационных качеств блочных шифраторов совсем не обязательно матрицы в XSL-схемах выбирать максимально рассеивающими. В некоторых ситуациях удачным компромиссом являются XSPL-схемы.

В следующем разделе вычисляется показатель θ для XSPL-схем с длиной блока $n = mk^2$. Коммутации в них (см. раздел 1) переставляют m -векторы по равномерно рассеивающим подстановкам степени k^2 , а матрицы $L_i \in GL(mk^2, 2)$ являются блочно-диагональными с k максимально рассеивающими блоками — матрицами из $GL(mk, 2)$.

Построение максимально рассеивающих матриц является сложным вопросом. Обнаружение каждой принципиально новой такой матрицы, тем более их семейства, является событием в криптографическом синтезе. Новыми считаются те матрицы, которые не получаются из известных перестановками полос, перестановками колонок и элементарными преобразованиями над строками внутри каждой полосы и над столбцами внутри каждой колонки.

Одно семейство максимально рассеивающих матриц, указанное авторам А. А. Дмухом, строится по матрицам Коши. Они задаются семейством из $2k$ различных элементов $a_1, \dots, a_k, b_1, \dots, b_k$ поля $GF(2^m)$. Известно (см., например, [15]), что $\det \|(a_i + b_j)^{-1}\|_{i,j=1,\dots,k} \neq 0$. Заменяя элементы $c_{ij} = (a_i + b_j)^{-1}$ на матрицы $\hat{c}_{ij} \in GL(m, 2)$, отвечающие в каком-либо базисе $GF(2^m)$ над $GF(2)$ линейному отображению $x \mapsto xc_{ij}$, $x \in GF(2^m)$, получим максимально рассеивающую матрицу из $GL(mk, 2)$. Такие матрицы используются в [16].

В монографии [2] можно найти описание последовательности этапов происхождения XSL-шифров, аналогичное приведенному в этом разделе.

3. Показатель рассеивания XSPL-шифра с длиной блока $n = mk^2$

Подробно XSPL-схемы, о которых пойдет речь, описаны в разделе 1. В данном разделе для них доказывается следующая теорема.

Теорема 3.1. Для XSPL-схемы с $r \geq 1$ итерациями, одна итерация которой преобразует блоки из $V_{m \cdot k^2}$ путем:

- прибавления итерационного ключа из $V_{m \cdot k^2}$ по mod 2,
- применения k^2 локальных перемешивающих подстановок из S_{V_m} ,

- умножения на блочно-диагональную матрицу из $GL(mk^2, 2)$ с k максимально рассеивающими блоками из $GL(mk, 2)$,
- перестановки m -векторов блока по равномерно рассеивающей подстановке из S_{k^2} ,

показатель рассеивания $\theta = \theta(r)$ линейной среды вычисляется по формулам $\theta(1) = 1, \theta(2) = k + 1, \theta(3) = 2k + 1, \theta(4) = (k + 1)^2, \theta(r) = (k + 1)^2 \left\lceil \frac{r-1}{4} \right\rceil + \theta\left(r - 4 \left\lceil \frac{r-1}{4} \right\rceil\right), \quad r \geq 5$.

Доказательство данной теоремы, хоть и не столь изящное, можно было бы построить на основе оценок и подхода из монографии [2]. Приводимое ниже доказательство отличается оригинальным графическим представлением XSLP-шифров, которое может быть использовано в будущем для оценок показателей рассеивания линейной среды таких шифров для $n = mk^r, r > 2$, и равномерно рассеивающих подстановок из S_{k^r} , построенных на основе обобщенных графов де Брейна [9].

Доказательство. Пусть $\mathcal{L} = ((l'_{ij}, l''_{ij}), i = 1, \dots, r, j = 0, 1, \dots, k^2 - 1)$ — произвольный ненулевой согласованный набор столбцов без дефектов, входящий в определение (6) показателя θ . Столбец l'_{ij} состоит из m бит меток входов подстановки π_{ij} , а столбец l''_{ij} состоит из m бит меток выходов этой же подстановки. Хотя бы один из этих $2rk^2$ столбцов ненулевой. Отсутствие дефектов означает, что $l'_{ij} = 0 \Leftrightarrow l''_{ij} = 0$ для всех $i = 1, 2, \dots, r, j = 0, 1, \dots, k^2 - 1$. Наконец, согласованность $\mathcal{L}$ означает, что

$$l''_i = L_i \cdot \hat{P}_i \cdot l'_{i+1}, \quad i = 1, 2, \dots, r - 1. \quad (7)$$

В равенстве (7) столбец l''_i составлен из столбцов $l''_{ij}, j = 0, 1, \dots, k^2 - 1$, столбец l'_{i+1} составлен из $l'_{i+1,j}, j = 0, 1, \dots, k^2 - 1, L_i \in GL(mk^2, 2)$ — блочно-диагональная матрица, составленная из k максимально рассеивающих блоков $B_{i,j_1} \in GL(mk, 2), j_1 = 0, 1, \dots, k-1, \hat{P}_i \in GL(mk^2, 2)$ — подстановочная матрица, осуществляющая коммутацию m -векторов и отвечающая равномерно рассеивающей подстановке $P_i: \{0, 1, \dots, k^2 - 1\} \rightarrow \{0, 1, \dots, k^2 - 1\}$. Без ограничения общности можно считать $P_i(j_0, j_1) = (j_1, j_0)$. При этом только, как и для SP-сетей (2) в разделе 2, меняются местами подстановки $\pi_{i,(0,j_1)}, \pi_{i,(1,j_1)}, \dots, \pi_{i,(m-1,j_1)}$ при всех $i = 1, \dots, r, j_1 = 0, 1, \dots, m-1$. Меняются местами также m полос из m подряд идущих строк и m колонок из m подряд идущих столбцов в блоках $B_{ij_1}, i = 1, \dots, r, j_1 = 0, 1, \dots, m-1$.

Для наших целей оказалось удобным графическое представление шифрпреобразования XSLP-схемы, приведенное на рисунке ниже. (Представлена схема при $k = 5$.)

Рис. Графическое представление шифрпреобразования XSLP-схемы ($k=5$)

В i -м ярусе каждый квадратик представляет блок B_{i,j_1} , $i = 1, 2, \dots, r$, $j_1 = 0, 1, \dots, k-1$. Между ярусами i , $i+1$ каждый блок B_{i,j'_1} соединен отрезками со всеми блоками B_{i,j''_1} , $j'_1, j''_1 = 0, 1, \dots, k-1$. По каждому отрезку $[B_{i,j'_1}, B_{i,j''_1}]$ проходит (сверху вниз) m -вектор, при этом он (по мере прохождения по отрезку) изменяется по подстановке $\pi_{i+1,(j'_1,j''_1)}$, к аргументу которой предварительно прибавляется (покоординатно по $\bmod 2$) m -вектор $z_{i+1,(j'_1,j''_1)} \in V_m$ итерационного ключа $z_{i+1} \in V_n$.

Набору $\mathcal{L}$ поставим в соответствие неориентированный граф Γ . (Фрагмент примера такого графа представлен на рисунке.) Вершинами графа Γ , располагающимися в следующих сверху вниз $r-1$ ярусах, являются те блоки B_{i,j_1} , $i = 1, \dots, r-1$, $j_1 = 0, 1, \dots, k-1$, для которых $l''_{i,*j_1} \neq 0$, а значит, и $l'_{i,*j_1} \neq 0$. Здесь столбец $l''_{i,*j_1}$ (соответственно, $l'_{i,*j_1}$) составлен из столбцов $l''_{i,(j_0,j_1)}$ (соответственно, $l'_{i,(j_0,j_1)}$), $j_0 = 0, 1, \dots, k-1$. Если $l'_{i+1,(j_0,j_1)} \neq 0$, $i = 1, \dots, r-2$, то вершину B_{i,j_0} из i -го яруса соединяем ребром с вершиной B_{i+1,j_1} из $(i+1)$ -го яруса. На рисунке ребра изображены утолщенными отрезками. Ребрами являются те отрезки, для которых хотя бы одна пометка соответствующего m -вектора ненулевая.

Дополнительно к каждой вершине B_{1,j_1} верхнего яруса сверху подрисовываем $[[l''_{1,*j_1}]] = |\{j_0 = 0, 1, \dots, k-1 : l''_{1,(j_0,j_1)} \neq 0\}|$ ребер, а к каждой вершине B_{r-1,j_1} нижнего яруса снизу подрисовываем $[[B_{r-1,j_1}^{-1} l''_{r-1,*j_1}]]$ ребер. После этого величина $\theta_{\mathcal{L}}$ будет совпадать с числом ребер в графе Γ .

В каждом ярусе имеется хотя бы одна вершина графа Γ . Иначе в силу (7) при отсутствии дефектов в наборе $\mathcal{L}$ все столбцы были бы нулевыми.

От каждой вершины B_{i,j_1} вверх отходит $[[l''_{i,*j_1}]]$ ребер. Число ребер, отходящих вниз от вершин B_{i,j_1} , равно числу цифр $j_0 \in \{0, 1, \dots, k-1\}$, для которых m -вектор с номером (j_0, j_1) в столбце $\hat{P}_i l''_{i+1}$ ненулевой. Согласно (7) это число равно $[[B_{i,j_1}^{-1} l''_{i,*j_1}]]$. Блок B_{i,j_1} максимально рассеивающий, поэтому от него отходит не менее $k+1$ ребер, поскольку $[[l''_{i,*j_1}]] + [[B_{i,j_1}^{-1} l''_{i,*j_1}]] \geq k+1$.

Ненулевой набор $\mathcal{L}$ без дефектов, для которого $\theta_{\mathcal{L}}$ совпадает с величиной $\theta(r)$ из формулировки теоремы, можно построить при каждом $r \geq 1$. Для этого нужно ориентироваться на получение графа Γ , в котором последовательность чисел вершин в ярусах является отрезком длины $r-1$ в бесконечной последовательности $\dots, 1, 1, k, k, \dots$ с периодом 4. Именно такой пример представлен на рисунке. Справа там указано отвечающее этому примеру число ребер между ярусами графа Γ (в общем случае для произвольного $k > 1$).

Неравенство

$$\theta_{\mathcal{L}} \geq \theta(r) \quad (8)$$

докажем индукцией по r , помня, что $\theta_{\mathcal{L}}$ равно числу ребер в графе Γ . В справедливости индуктивного перехода убеждаемся после удаления вершин четвертого сверху яруса в графе Γ , оставляя при этом инцидентные им ребра (как сверху, так и снизу). Действительно, тогда исходный граф с $r-1$ ярусами вершин распадется на два графа. Число ярусов нижнего графа будет равно $r''-1 = r-1-4 = r-5$. Он отвечает XSLP-схеме с $r'' = r-4$ итерациями. В верхнем графе будет $r'-1 = 3$ яруса, которые отвечают XSLP-схеме с $r' = 4$ итерациями. Произвольный ненулевой согласованный набор столбцов без дефектов $\mathcal{L}$ для исходной XSLP-схемы будет индуцировать аналогичные наборы $\mathcal{L}'$ и $\mathcal{L}''$ соответственно для верхней и нижней XSLP-схем, при этом $\theta_{\mathcal{L}} = \theta_{\mathcal{L}'} + \theta_{\mathcal{L}''}$. По предположению индукции тогда имеем: $\theta_{\mathcal{L}} = \theta_{\mathcal{L}'} + \theta_{\mathcal{L}''} \geq \theta(4) + \theta(r-4) = (m+1)^2 + \theta(r-4) = \theta(r)$. Для доказательства теоремы остается убедиться в справедливости базы индукции. При $r = 1$ и $r = 2$ неравенство (8) очевидно. Осталось его проверить для $r = 3$ и $r = 4$. При $r = 3$ через $q_1 \geq 1$ и $q_2 \geq 1$ обозначим числа вершин соответственно в первом и втором ярусах. Если в Γ нет ребра, соединяющего вершину A из первого яруса и вершину B из второго яруса, то мы его проведем, но одновременно удалим одно ребро над вершиной A (их было не меньше двух). В полученном графе число ребер не увеличилось, и по-прежнему каждая вершина смежна не менее чем с $k+1$ ребрами.

Поэтому можно считать, что каждая вершина первого яруса соединена со

всеми вершинами второго яруса. Тогда $\theta_{\mathcal{L}} \geq q_1 q_2 + q_1(k+1-q_2) + q_2(k+1-q_1) = (k+1)(q_1+q_2) - q_1 q_2 \geq 2k+1$.

При $r = 4$ через $q_1 \geq 1$, $q_2 \geq 1$ и $q_3 \geq 1$ обозначим числа вершин в первом, втором и третьем ярусах соответственно. Снова считаем, что все пары вершин соседних ярусов смежны. Тогда $\theta_{\mathcal{L}} \geq q_1(k+1-q_2) + q_1 q_2 + q_2 q_3 + q_3(k+1-q_2) = (q_1+q_3)(k+1) \geq (k+1)^2$. Теорема доказана. $\square$

Аналогичный показатель рассеивания θ' линейной среды шифрпреобразования может быть определен и относительно разностного метода криптографического анализа (см. [12]). Установленная там двойственность между линейным и разностным методами в случае XSLP-сети позволяет утверждать, что справедливо равенство $\theta' = \theta$.

Список литературы

- [1] Daemen J., *Cipher and hash function design strategies based on linear and differential cryptanalysis*, Doct. Diss., K.U.Leuven, 1995.
- [2] Daemen J., Rijmen V., *The Design of Rijndael: AES — The Advanced Encryption Standard*, Heidelberg etc.: Springer, 2002.
- [3] Rijmen V., *Cryptanalysis and design of iterated block ciphers*, Doct. Diss., K.U.Leuven, 1997.
- [4] Шеннон К., *Работы по теории информации и кибернетике*, М.: ИЛ, 1963.
- [5] Диффи У., Хеллман М.Е., “Защищённость и имитостойкость: Введение в криптографию”, *ТИИЭР*, **67**:3 (1979), 71–109.
- [6] Мессеи Дж. Л., “Введение в современную криптологию”, *ТИИЭР*, **76**:5 (1988), 24–42.
- [7] Хоффман Л. Дж., *Современные методы защиты информации*, М.: Советское радио, 1980.
- [8] Шнайер Б., *Прикладная криптография*, М.: ТРИУМФ, 2003.
- [9] Малышев Ф.М., Тараканов В.Е., “Обобщённые графы де Брейна”, *Матем. заметки*, **62**:4 (1997), 540–548.
- [10] Matsui M., “Linear Cryptanalysis Method for DES Cipher”, *Lect. Notes Comput. Sci.*, **765**, 1994, 24–27.
- [11] Biham E., Shamir A., “Differential cryptanalysis of DES-like cryptosystem”, *Lect. Notes Comput. Sci.*, **537**, 1991, 2–21.
- [12] Малышев Ф.М., “Двойственность разностного и линейного методов в криптографии”, *Математические вопросы криптографии*, **5**:3 (2014), 35–48.
- [13] Matsui M., “On correlation between the order of S -boxes and the strength of DES”, *Lect. Notes Comput. Sci.*, **950**, 1995, 366–375.
- [14] Rijmen V., Daemen J., Preneel B., Bosselaers A., De Win E., “The cipher SHARK”, *Lect. Notes Comput. Sci.*, **1039**, 1996, 99–111.
- [15] Проскуряков И.В., *Сборник задач по линейной алгебре*, 6-е изд., М.: Наука, 1978.
- [16] Youssef A.M., Misters S., Tavares S.E., “The design of linear transformations for substitution permutation encryption networks”. In: *Workshop On Selected Areas in Cryptography (SAC'96): Workshop Record*, 1997, 40–48.