Math-Net.Ru

Общероссийский математический портал

В. А. Федченко, Минимальные согласованные системы локальных вероятностных соотношений в AES-подобных алгоритмах шифрования, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 3, 127–142

DOI: <https://doi.org/10.4213/mvk266>

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: 3.89.185.249

26 апреля 2023 г., 12:33:50

**Минимальные согласованные системы
локальных вероятностных соотношений
в AES-подобных алгоритмах шифрования**

В. А. Федченко

Белорусский государственный университет, Минск, Беларусь

Получено 06.III.2018

Аннотация. В терминах теоретико-графовой модели дано исчерпывающее описание согласованных систем локальных линейных (разностных) вероятностных соотношений с наименьшим числом активных S-блоков для AES-подобных алгоритмов шифрования с произвольным числом итераций, с равномерно рассеивающими перестановками и локальными матрицами с фиксированным линейным (разностным) коэффициентом рассеивания.

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

**Minimal consistent systems of local probabilistic relations
for AES-like ciphers**

V. A. Fedchenko

Belarusian State University, Minsk, Belarus

Abstract. In terms of graph-theoretical model we give a complete description of consistent systems of linear (differential) probabilistic relations with minimum number of active S-boxes for AES-like cipher with arbitrary number of rounds, uniformly diffusive permutations and fixed linear (differential) branch numbers of local matrices.

Key words: AES, AES-like algorithm, XSLP-cipher, linear cryptanalysis, differential cryptanalysis, active S-box, linear (differential) trail

1.

В [1] в качестве модели для исследования AES-подобных алгоритмов шифрования используется *XSLP-шифр* с $r \in \mathbb{N}$ итерациями и размером блока $n = mk^2$ битов, $n, m, k \in \mathbb{N}$ [2]. Напомним, что каждая итерация XSLP-шифра представляет собой суперпозицию наложения итерационного ключа (X) побитово по модулю 2, замены m -векторов (из $V_m = \text{GF}(2)^m$) посредством локальных подстановок (S), умножения mk -векторов на матрицы (L) и перестановки m -векторов (P).

В связи с линейным и разностным методами анализа XSLP-шифров возникает комбинаторная задача составления *согласованных систем локальных линейных (разностных) соотношений*, выполняющихся с наибольшей вероятностью (см. [2, 1]). Как правило, такие системы должны быть *минимальными*, т. е. содержать наименьшее возможное число *активных S-блоков* — локальных подстановок, для которых в системе присутствуют ненулевые линейные (разностные) вероятностные соотношения. Это наименьшее число определяется свойствами линейных преобразований XSLP-шифра и называется линейным (разностным) *показателем рассеивания линейной среды* [2].

При исследовании показателей рассеивания линейной среды XSLP-шифров в [1] вводится определение *r -слойного графа*, $r \in \mathbb{N}$, соответствующего усеченному представлению системы локальных линейных (разностных) вероятностных соотношений для XSLP-шифра. По определению r -слойный граф состоит из r слоев вершин и $r + 1$ слоев направленных ребер (дуг). Вершины соответствуют локальным матрицам XSLP-шифра, для которых в согласованной системе присутствуют ненулевые соотношения. Ребра соответствуют ненулевым m -векторам в локальных соотношениях, а также отражают их переходы под действием перестановочных преобразований. Из каждой вершины i -го слоя могут выходить дуги только в вершины $(i + 1)$ -го слоя, $i = 1, 2, \dots, r - 1$. В вершины 1-го слоя входят дуги, не имеющие начала. Из вершин r -го слоя выходят дуги, не имеющие окончания. Заметим, что общее число ребер, входящих во все вершины графа, совпадает с числом активных S-блоков, что позволяет исследовать согласованные системы локальных линейных (разностных) вероятностных соотношений для XSLP-шифров исключительно на языке теории графов.

Для числовых характеристик i -го слоя r -слойного графа, $i = 1, 2, \dots, r$, $r \in \mathbb{N}$, вводятся следующие обозначения:

$q_i \in \mathbb{N}$ — количество вершин в i -м слое,

$D_i^\downarrow = (d_{i,1}^\downarrow, d_{i,2}^\downarrow, \dots, d_{i,q_i}^\downarrow)$ — набор степеней захода вершин i -го слоя,

$D_i^\uparrow = (d_{i,1}^\uparrow, d_{i,2}^\uparrow, \dots, d_{i,q_i}^\uparrow)$ — набор степеней исхода вершин i -го слоя,

$D_i = (d_{i,1}, d_{i,2}, \dots, d_{i,q_i})$ — набор степеней вершин i -го слоя,

$d_{i,j} = d_{i,j}^\downarrow + d_{i,j}^\uparrow, j = 1, 2, \dots, q_i,$

$s_i = \sum_{j=1}^{q_i} d_{i,j}^\downarrow, s_{r+1} = \sum_{j=1}^{q_r} d_{r,j}^\uparrow.$

Основные условия, накладываемые на r -слойные графы по определению, выражаются в следующем:

$$q_i \geq 1, \quad i = 1, 2, \dots, r, \quad (1)$$

$$d_{i,j}^\downarrow \geq 1, d_{i,j}^\uparrow \geq 1 \text{ для всех } j = 1, \dots, q_i, i = 1, 2, \dots, r. \quad (2)$$

Если r -слойные графы используются для исследования XSLP-шифров с равномерно рассеивающими перестановками [2] и локальными матрицами с фиксированным линейным (разностным) коэффициентом рассеивания $\rho \in \mathbb{N}, \rho \geq 2$ (см. [1]), то также должно быть выполнено:

$$d_{i,j} \geq \rho \text{ для всех } j = 1, \dots, q_i, i = 1, 2, \dots, r, \quad (3)$$

$$\begin{aligned} &\text{каждая вершина } i\text{-го слоя может быть соединена дугой} \\ &\text{с произвольной вершиной } (i+1)\text{-го слоя не более одного раза.} \end{aligned} \quad (4)$$

Множество всех попарно неизоморфных r -слойных графов, удовлетворяющих условиям (1)–(4), обозначим $G(\rho, r)$.

Пример 1. На рис. 1 [19] $r = 3$ итерации XSLP-шифра с размером блока $n = m \cdot 3^2, m \in \mathbb{N}$, с равномерно рассеивающими перестановками и локальными матрицами с фиксированным линейным (разностным) коэффициентом рассеивания $\rho = 3$. На схеме показана некоторая согласованная система локальных линейных (разностных) вероятностных соотношений (утолщенными линиями выделены активные S-блоки, локальные матрицы и m -векторы). Представлен соответствующий 3-слойный граф $\Gamma^{(3)} \in G(3, 3)$.

На рис. 1 $z_{i,j} \in V_m$ — элементы итерационных ключей, $\pi_{i,j} \in S_{V_m}$ — локальные подстановки, $B_{i,j} \in \text{GL}(3m, 2)$ — локальные матрицы.

Рис. 1. Представления согласованной системы локальных линейных (разностных) вероятностных соотношений для XSLLP-шифра с длиной блока $n = m \cdot 3^2$

Естественный интерес представляют *реберно минимальные* r -слойные графы $\Gamma^{(r)} \in G(\rho, r)$, для которых количество ребер $S(\Gamma^{(r)}) = s_1 + s_2 + \dots + s_r$ является наименьшим:

$$S(\Gamma^{(r)}) = \min_{\Gamma_1^{(r)} \in G(\rho, r)} S(\Gamma_1^{(r)}) =: S_{\min}(\rho, r). \quad (5)$$

Множество реберно минимальных r -слойных графов из $G(\rho, r)$ обозначим $G_{\min}(\rho, r)$. В [1] получено точное значение величины $S_{\min}(\rho, r)$ при любых $\rho \geq 2$ и $r \geq 1$.

Теорема 1 ([1]). Пусть $\Gamma^{(r)} \in G_{\min}(\rho, r)$ — реберно минимальный r -слойный граф. Тогда $S(\Gamma^{(r)}) = S_{\min}(\rho, r)$, при этом

$$S_{\min}(\rho, r) = \begin{cases} 1, & \text{если } r = 1, \\ \rho, & \text{если } r = 2, \\ 2\rho - 1, & \text{если } r = 3, \\ \rho^2, & \text{если } r = 4, \\ S_{\min}(\rho, r-4) + \rho^2, & \text{если } r > 4. \end{cases} \quad (6)$$

2.

В настоящей работе рассматривается вопрос перечисления реберно минимальных r -слойных графов. Данный вопрос интересен в связи с тем, что в общем случае не для каждого реберно минимального r -слойного графа может найтись соответствующая согласованная система локальных линейных (разностных) соотношений для r итераций XSLP-шифра, так как теоретико-графовая модель не учитывает реальную возможность выполнения соотношений для локальных матриц, представляя их в виде абстрактных вершин с некоторым количеством входящих и исходящих дуг. Перечисление всех реберно минимальных r -слойных графов может позволить найти граф, для которого соответствующая система существует.

Заметим, что мощности множеств $G(\rho, r)$ и $G_{\min}(\rho, r)$ заведомо не ограничены сверху, так как, в частности, условиями (1)–(4) не установлена граница сверху для степеней исхода вершин r -го слоя. В связи с этим определим множество

$$G(\rho, r, k), \quad k \in \mathbb{N}, \quad k \geq \rho - 1,$$

графов из $G(\rho, r)$, удовлетворяющих условиям

$$\begin{aligned} q_i &\leq k \quad \text{для всех } i \in \overline{1, r}, \\ d_{i,j}^{\downarrow} &\leq k \text{ и } d_{i,j}^{\uparrow} \leq k \quad \text{для всех } i \in \overline{1, r}, \quad j \in \overline{1, q_i}. \end{aligned} \quad (7)$$

(Обратим внимание на то, что неравенства $d_{i,j}^{\downarrow} \leq k$ для $i \in \overline{2, r}$ и неравенства $d_{i,j}^{\uparrow} \leq k$ для $i \in \overline{1, r-1}$ следуют из (4) и верхнего неравенства в (7).) Соответствующее множество реберно минимальных графов (рассматриваемых с точностью до изоморфизма) обозначим $G_{\min}(\rho, r, k)$. Ограничения (7) естественным образом возникают при исследовании XSLP-шифров с размером блока $n = mk^2$. Условие $k \geq \rho - 1$ обосновано неравенствами $2 \leq \rho \leq k + 1$ для коэффициента рассеивания локальных матриц (см. [2, 3]).

Ввиду отмеченной неопределенности в последнем слое ребер перечисление элементов множества $G_{\min}(\rho, r)$ в некоторых случаях можно производить без учета этого слоя. Будем считать графы из $G(\rho, r)$ эквивалентными с точностью до последнего слоя ребер, если они оказываются изоморфными после удаления ребер, исходящих из вершин r -го слоя. Множества попарно не эквивалентных представителей из $G(\rho, r)$ и $G_{\min}(\rho, r)$ обозначим $\tilde{G}(\rho, r)$ и $\tilde{G}_{\min}(\rho, r)$ соответственно.

Будем говорить, что r -слойный граф $\Gamma^{(r)} \in G(\rho, r)$ представлен в виде последовательного объединения r_1 -слойного графа $\Gamma_1^{(r_1)} \in G(\rho, r_1)$ и r_2 -слойного графа $\Gamma_2^{(r_2)} \in G(\rho, r_2)$, $r_1, r_2 \in \mathbb{N}_0$, $r_1 + r_2 = r$, если граф $\Gamma_1^{(r_1)}$ состоит из первых r_1 слоев вершин графа $\Gamma^{(r)}$ и инцидентных им ребер, граф $\Gamma_2^{(r_2)}$ состоит из последних r_2 слоев вершин графа $\Gamma^{(r)}$ и инцидентных им ребер. Указанное представление обозначим следующим образом:

$$\Gamma^{(r)} = \Gamma_1^{(r_1)} \cup \Gamma_2^{(r_2)}.$$

Заметим, что графы $\Gamma_1^{(r_1)}$ и $\Gamma_2^{(r_2)}$ имеют общий слой ребер, т. е. ребра, выходящие из вершин r_1 -го слоя графа $\Gamma_1^{(r_1)}$, одновременно являются ребрами, входящими в вершины 1-го слоя графа $\Gamma_2^{(r_2)}$. Граф $\Gamma^{(0)}$, обладающий свойством

$$\Gamma^{(r)} = \Gamma^{(0)} \cup \Gamma^{(r)} = \Gamma^{(r)} \cup \Gamma^{(0)}, \quad r \geq 0,$$

будем считать «пустым». Естественным образом определяется понятие представления некоторого графа $\Gamma^{(r)} \in G(\rho, r)$ в виде последовательного объединения $t \in \mathbb{N}$ графов

$$\Gamma_1^{(r_1)} \in G(\rho, r_1), \dots, \Gamma_t^{(r_t)} \in G(\rho, r_t), \quad r_1, \dots, r_t \in \mathbb{N}_0, \quad r_1 + \dots + r_t = r.$$

Утверждение 1. *Произвольный реберно минимальный r -слойный граф $\Gamma^{(r)} \in G_{\min}(\rho, r)$ может быть представлен в виде последовательного объединения одного реберно минимального $\{\frac{r}{4}\}$ -слойного графа и $\lceil \frac{r}{4} \rceil$ реберно минимальных 4-слойных графов, где $\{\frac{r}{4}\}$ — остаток от деления r на 4, $\lceil \frac{r}{4} \rceil$ — целая часть числа $\frac{r}{4}$.*

Доказательство. Применим метод математической индукции по r . При $1 \leq r \leq 4$ доказательство очевидно. Пусть $r > 4$, рассмотрим произвольный реберно минимальный r -слойный граф $\Gamma^{(r)} \in G_{\min}(\rho, r)$. Представим его в виде последовательного объединения одного $\{\frac{r}{4}\}$ -слойного графа (возможно, «пустого») и $\lceil \frac{r}{4} \rceil$ 4-слойных графов:

$$\Gamma^{(r)} = \Gamma^{(\{\frac{r}{4}\})} \cup \Gamma_1^{(4)} \cup \Gamma_2^{(4)} \cup \dots \cup \Gamma_{\lceil \frac{r}{4} \rceil - 1}^{(4)} \cup \Gamma_{\lceil \frac{r}{4} \rceil}^{(4)}.$$

Предположим, что граф $\Gamma_{\lfloor \frac{r}{4} \rfloor}^{(4)}$ не является реберно минимальным, тогда $S(\Gamma_{\lfloor \frac{r}{4} \rfloor}^{(4)}) > \rho^2$. Полагая

$$\Gamma^{(r-4)} = \Gamma(\{\frac{r}{4}\}) \cup \Gamma_1^{(4)} \cup \dots \cup \Gamma_{\lfloor \frac{r}{4} \rfloor - 1}^{(4)},$$

находим:

$$\begin{aligned} S(\Gamma^{(r-4)}) &= S(\Gamma^{(r)}) - S(\Gamma^{(4)}) < \\ &< S_{\min}(\rho, r) - \rho^2 = S_{\min}(\rho, r - 4), \end{aligned}$$

что противоречит теореме 1. Полученное противоречие доказывает, что граф $\Gamma_{\lfloor \frac{r}{4} \rfloor}^{(4)}$ является реберно минимальным и $S(\Gamma_{\lfloor \frac{r}{4} \rfloor}^{(4)}) = \rho^2$. Следовательно,

$$S(\Gamma^{(r-4)}) = S_{\min}(\rho, r - 4)$$

и граф $\Gamma^{(r-4)}$ также является реберно минимальным, что позволяет применить предположение индукции.

Утверждение 1 доказано. $\square$

3.

Перечисление реберно минимальных r -слойных графов сводится к перечислению реберно минимальных 1-, 2-, 3- и 4-слойных графов, а также способов их последовательного объединения.

Утверждение 2. Для любого реберно минимального 1-слойного графа $\Gamma^{(1)} \in G_{\min}(\rho, 1)$ справедливы соотношения

$$q_1 = 1, \quad d_{1,1} \geq \rho, \quad d_{1,1}^\downarrow = 1, \quad d_{1,1}^\uparrow \geq \rho - 1. \quad (8)$$

Количество реберно минимальных 1-слойных графов вычисляется по формулам

$$|\tilde{G}_{\min}(\rho, 1)| = 1, \quad (9)$$

$$|G_{\min}(\rho, 1, k)| = k - \rho + 2. \quad (10)$$

Доказательство. Справедливость (8) очевидна ввиду теоремы 1. Из (8) следует (9), т.е. существует единственный с точностью до последнего слоя реберно минимальный 1-слойный граф. Графы из $G_{\min}(\rho, 1, k)$ могут иметь $d_{1,1}^\uparrow = \rho - 1, \rho, \dots, k$, $k \geq \rho - 1$, ребер в последнем слое, что обосновывает формулу (10).

Утверждение 2 доказано. $\square$

Утверждение 3. Для любого реберно минимального 2-слойного графа $\Gamma_{\min}^{(2)} \in G(\rho, 2)$ справедливы соотношения

$$\begin{aligned} q_1 = 1, \quad d_{1,1} = d_{1,1}^\downarrow + d_{1,1}^\uparrow = \rho, \quad 1 \leq d_{1,1}^\downarrow \leq \rho - 1, \quad 1 \leq d_{1,1}^\uparrow \leq \rho - 1, \\ q_2 = d_{1,1}^\uparrow = \rho - d_{1,1}^\downarrow, \quad d_{2,j}^\downarrow = 1, \quad d_{2,j}^\uparrow \geq \rho - 1 \quad \text{для всех } j \in \overline{1, q_2}. \end{aligned} \quad (11)$$

Количество реберно минимальных 2-слойных графов вычисляется по формулам

$$|\tilde{G}_{\min}(\rho, 2)| = \rho - 1, \quad (12)$$

$$|G_{\min}(\rho, 2, k)| = \sum_{r=1}^{\rho-1} C_{r+k-\rho+1}^r. \quad (13)$$

Доказательство. По теореме 1 количество ребер в двух верхних слоях любого реберно минимального 2-слойного графа равно ρ . С учетом условия (3) это количество может быть достигнуто только при $q_1 = 1$, $d_{1,1} = \rho$. Вместе с тем существует $\rho - 1$ способов распределения ρ ребер между заходящими и выходящими из единственной вершины, что обосновывает формулу (12). При этом первые два слоя любого реберно минимального 2-слойного графа однозначно определяются значением $d_{1,1}^\downarrow \in \{1, 2, \dots, \rho - 1\}$ по формулам (11).

Из формул (11) следует, что для каждого фиксированного $q_2 \in \{1, 2, \dots, \rho - 1\}$ существует единственный с точностью до последнего слоя реберно минимальный 2-слойный граф, при этом $d_{2,j}^\uparrow \geq \rho - 1$ для всех $j \in \overline{1, q_2}$. Пусть также $d_{2,j}^\uparrow \leq k$ для всех $j \in \overline{1, q_2}$ при некотором $k \geq \rho - 1$.

При фиксированном $q_2 \in \{1, 2, \dots, \rho - 1\}$ каждый граф из $G_{\min}(\rho, 2, k)$ однозначно определяется неупорядоченным множеством степеней исхода вершин 2-го слоя:

$$\{d_{2,1}^\uparrow, \dots, d_{2,q_2}^\uparrow\}, \quad (14)$$

где $d_{2,j}^\uparrow = \rho - 1, \rho, \dots, k$, $j = 1, 2, \dots, q_2$, $q_2 = 1, 2, \dots, \rho - 1$. Количество таких множеств равно числу сочетаний с повторениями из $n = k - \rho + 2$ элементов по $r = q_2$, которое равно

$$C_{n+r-1}^r = C_{q_2+k-\rho+1}^{q_2}$$

(см. [4, с. 11]). Суммируя по всем допустимым значениям q_2 , получаем формулу (13).

Утверждение 3 доказано. $\square$

Утверждение 4. Для любого реберно минимального 3-слойного графа $\Gamma_{\min}^{(3)} \in G(\rho, 3)$ справедливы соотношения

$$\begin{aligned} q_1 &= 1, & d_{1,1} &= \rho, & d_{1,1}^\downarrow &= \rho - 1, & d_{1,1}^\uparrow &= 1, \\ q_2 &= 1, & d_{2,1} &= \rho, & d_{2,1}^\downarrow &= 1, & d_{2,1}^\uparrow &= \rho - 1, \\ q_3 &= \rho - 1, & d_{3,j}^\downarrow &= 1, & d_{3,j}^\uparrow &\geq \rho - 1 & \text{ для всех } j &\in \overline{1, q_3}. \end{aligned} \quad (15)$$

Количество реберно минимальных 3-слойных графов вычисляется по формулам

$$|\tilde{G}_{\min}(\rho, 3)| = 1, \quad (16)$$

$$|G_{\min}(\rho, 3, k)| = C_k^{\rho-1}. \quad (17)$$

Доказательство. Покажем, что $q_1 = q_2 = 1$ для любого $\Gamma^{(3)} \in G_{\min}(\rho, 3)$. Так как $s_3 \geq q_2 \geq 1$, $s_1 \geq q_1 \geq 1$, то

$$2\rho - 1 \stackrel{(6)}{=} \sum_{j=1}^{q_1} d_{1,j} + s_3 \stackrel{(3)}{\geq} q_1 \rho + 1, \quad 2\rho - 1 \stackrel{(6)}{=} s_1 + \sum_{j=1}^{q_2} d_{2,j} \stackrel{(3)}{\geq} q_2 \rho + 1,$$

откуда $q_1 \leq 2 - 2/\rho$ и $q_2 \leq 2 - 2/\rho$, поэтому $q_1 = 1$, $q_2 = 1$ ввиду условия $\rho \geq 2$. Отсюда очевидным образом следуют формулы (15) и (16). Формула (17) получается аналогично (13) как число сочетаний с повторениями из $k - \rho + 2$ элементов по $r = q_3 = \rho - 1$, которое равно $C_{n+r-1}^r = C_{k-\rho+2+\rho-1-1}^r = C_k^{\rho-1}$ (см. [4, с. 11]).

Утверждение 4 доказано. $\square$

На рис. 2 представлены схематические изображения всех возможных реберно минимальных 1-, 2- и 3-слойных графов.

Рис. 2. Реберно минимальные 1-, 2- и 3-слойные графы

Утверждение 5. Для любого реберно минимального 4-слойного графа $\Gamma^{(4)} \in G_{\min}(\rho, 4)$ справедливы соотношения

$$q_i \leq \rho - 1, \quad i = 1, 2, 3, \quad (18)$$

$$q_1 + q_3 = \rho, \quad (19)$$

$$d_{i,1} = \dots = d_{i,q_i} = \rho, \quad i = 1, 2, 3, \quad (20)$$

$$d_{i,1}^\downarrow = \dots = d_{i,q_i}^\downarrow \stackrel{\text{def}}{=} d_i^\downarrow, \quad i = 1, 2, 3, \quad (21)$$

$$d_{i,1}^\uparrow = \dots = d_{i,q_i}^\uparrow \stackrel{\text{def}}{=} d_i^\uparrow, \quad i = 1, 2, 3, \quad (22)$$

$$d_i^\uparrow = q_{i+1}, \quad d_{i+1}^\downarrow = q_i, \quad i = 1, 2, \quad (23)$$

$$d_1^\downarrow = d_3^\uparrow = \rho - q_2. \quad (24)$$

Доказательство. Справедливы следующие неравенства:

$$\rho^2 \stackrel{(6)}{=} S(\Gamma^{(4)}) = \sum_{j=1}^{q_1} d_{1,j} + \sum_{j=1}^{q_3} d_{3,j} \stackrel{(3)}{\geq} (q_1 + q_3)\rho,$$

$$\rho^2 \stackrel{(6)}{=} S(\Gamma^{(4)}) = s_1 + \sum_{j=1}^{q_2} d_{2,j} + s_4 \stackrel{(3)}{\geq} 1 + q_2\rho + 1 > q_2\rho,$$

вследствие чего

$$q_1 + q_3 \leq \rho, \quad (25)$$

$$q_2 \leq \rho - 1. \quad (26)$$

Свойство (18) следует непосредственно из (1), (25) и (26).

Докажем свойство (19). С одной стороны, выполнено (25). С другой стороны, из (3) следует, что $d_{2,j} \geq \rho$ для всех $j \in \overline{1, q_2}$, поэтому каждая вершина 2-го слоя связана суммарно не менее чем с ρ вершинами 1-го и 3-го слоев. Отсюда $q_1 + q_3 \geq \rho$.

Перейдем к доказательству свойства (20). Непосредственно из (19) следует, что $d_{2,j} = \rho$ для всех $j \in \overline{1, q_2}$. Значит, любая вершина 1-го слоя связана со всеми вершинами 2-го слоя и любая вершина 2-го слоя связана со всеми вершинами 3-го слоя. Предположим, что существует такое $j \in \overline{1, q_1}$, что $d_{1,j} \geq \rho + 1$. С учетом (18) имеем $d_{1,j}^\downarrow \geq 2$. Тогда путем удаления «лишнего» ребра 1-го (самого верхнего) слоя можно получить некоторый 4-слойный граф, имеющий меньше ребер, чем граф $\Gamma^{(4)}$. Последнее противоречит реберной минимальности $\Gamma^{(4)}$. Значит, предположение не верно и $d_{1,j} = \rho$ для всех $j \in \overline{1, q_1}$. Аналогичными рассуждениями можно получить, что $d_{3,j} = \rho$ для всех $j \in \overline{1, q_3}$.

Свойства (21), (22), (23) и (24) следуют из обоснованной выше полной связности между слоями 1, 2 и 2, 3. Принимая это во внимание, имеем

$$d_{i,1}^{\uparrow} = \dots = d_{i,q_i}^{\uparrow} \quad \text{при } i = 1, 2$$

и

$$d_{i,1}^{\downarrow} = \dots = d_{i,q_i}^{\downarrow} \quad \text{при } i = 2, 3.$$

Отсюда с учетом свойства (20) легко получить

$$d_{1,1}^{\downarrow} = \dots = d_{1,q_1}^{\downarrow} = \rho - q_2$$

и

$$d_{3,1}^{\uparrow} = \dots = d_{3,q_3}^{\uparrow} = \rho - q_2.$$

Утверждение 5 доказано. $\square$

Замечание 1. Первые 3 слоя вершин и инцидентные им ребра реберно минимального 4-слойного графа однозначно определяются значениями $q_1, d_1^{\downarrow} \in \{1, 2, \dots, \rho - 1\}$. Таким образом, общее количество различных начальных участков из трех слоев в реберно минимальных 4-слойных графах равно $(\rho - 1)^2$. При этом по свойствам (19) и (24) имеем $q_3 = \rho - q_1$ и $d_3^{\uparrow} = d_1^{\downarrow}$. При формировании 4-го слоя вершин и ребер, как правило, возникает большая вариативность, так как существует много способов распределить $q_3 d_3^{\uparrow}$ дуг между q_4 вершинами со степенями захода $d_{4,1}^{\downarrow}, \dots, d_{4,q_4}^{\downarrow}$, где $d_3^{\uparrow} \leq q_4 \leq q_3 d_3^{\uparrow}$ и $1 \leq d_{4,j}^{\downarrow} \leq q_3$.

Замечание 2. Полная определенность при формировании 4-го слоя вершин и инцидентных им ребер в реберно минимальных 4-слойных графах имеет место в случае, когда $q_1 = \rho - 1$. Тогда $q_3 = 1$ в силу свойства (19), а в силу свойства (24), как уже отмечалось, $d_3^{\uparrow} = d_1^{\downarrow}$, где $d_1^{\downarrow} \in \{1, 2, \dots, \rho - 1\}$. Существует единственный способ провести $d_3^{\uparrow}$ ребер к вершинам 4-го слоя из единственной вершины 3-го слоя, следовательно,

$$q_4 = d_1^{\downarrow}, \quad d_{4,1}^{\downarrow} = \dots = d_{4,q_4}^{\downarrow} = 1. \quad (27)$$

Для степеней исхода вершин 4-го слоя в этом случае можно привести оценку снизу:

$$d_{4,j}^{\uparrow} \geq \rho - 1 \quad \text{для всех } j \in \overline{1, q_4}. \quad (28)$$

Пример 2. На рис. 3 представлены схематические изображения всех возможных реберно минимальных 4-слойных графов при $\rho = 4$.

Рис. 3. Реберно минимальные 4-слойные графы при $\rho = 4$

Лемма. Для любого реберно минимального r -слойного графа $\Gamma^{(r)} \in G_{\min}(\rho, r)$ при r , кратном 4 (т. е. при $\{\frac{r}{4}\} = 0$), и $q_1 = \rho - 1$:

$$\begin{aligned}
 d_{i,1}^{\downarrow} &= \dots = d_{i,q_i}^{\downarrow} \stackrel{\text{def}}{=} d_i^{\downarrow}, \quad i = 1, 2, \dots, r, \\
 d_{i,1}^{\uparrow} &= \dots = d_{i,q_i}^{\uparrow} = \rho - d_i^{\downarrow} \stackrel{\text{def}}{=} d_i^{\uparrow}, \quad i = 1, 2, \dots, r-1, \\
 d_{r,j}^{\uparrow} &\geq \rho - 1 \quad \text{для всех } j \in \overline{1, q_r}, \\
 d_i^{\uparrow} &= q_{i+1}, \quad d_{i+1}^{\downarrow} = q_i, \quad i = 1, 2, \dots, r-1,
 \end{aligned} \tag{29}$$

где $d_1^{\downarrow} \in \{1, 2, \dots, \rho - 1\}$.

Доказательство. По утверждению 1 граф $\Gamma^{(r)} \in G_{\min}(\rho, r)$ может быть представлен в виде последовательного объединения $t = r/4 > 0$ реберно минимальных 4-слойных графов: $\Gamma^{(r)} = \Gamma_1^{(4)} \cup \dots \cup \Gamma_t^{(4)}$, где $\Gamma_1^{(4)}, \dots, \Gamma_t^{(4)} \in G_{\min}(\rho, 4)$. Далее используем индукцию по t .

Если $t = 1$, то (29) обосновывается свойствами графа $\Gamma_1^{(4)}$ из утверждения 5 и из замечания 2. Если $t > 1$, то из (28) следует, что $q_5 \geq \rho - 1$. Вместе с тем по свойству (18) графа $\Gamma_2^{(4)}$ в графе $\Gamma^{(r)}$ имеем $q_5 \leq \rho - 1$. Следовательно, для графа $\Gamma^{(r)}$ справедливы равенства

$$\begin{aligned} d_{4,1}^{\uparrow} &= \dots = d_{4,q_4}^{\uparrow} = \rho - 1, \\ q_5 &= \rho - 1, \quad d_{5,1}^{\downarrow} = \dots = d_{5,q_5}^{\downarrow} = d_1^{\downarrow}, \quad d_{5,1}^{\uparrow} = \dots = d_{5,q_5}^{\uparrow} = \rho - d_1^{\downarrow}. \end{aligned} \quad (30)$$

Первый слой графа $\Gamma_2^{(4)}$ совпадает с первым слоем графа $\Gamma_1^{(4)}$, поэтому можно применять предположение индукции к графу $\Gamma^{(r-4)} = \Gamma_2^{(4)} \cup \dots \cup \Gamma_t^{(4)}$.

Лемма доказана. $\square$

Теорема 2. Для любого реберно минимального r -слойного графа $\Gamma^{(r)} \in G_{\min}(\rho, r)$ при $\{\frac{r}{4}\} = 1, 2, 3$

$$\begin{aligned} d_{i,1}^{\downarrow} &= \dots = d_{i,q_i}^{\downarrow} \stackrel{\text{def}}{=} d_i^{\downarrow}, \quad i = 1, 2, \dots, r, \\ d_{i,1}^{\uparrow} &= \dots = d_{i,q_i}^{\uparrow} = \rho - d_i^{\downarrow} \stackrel{\text{def}}{=} d_i^{\uparrow}, \quad i = 1, 2, \dots, r-1, \\ d_{r,j}^{\uparrow} &\geq \rho - 1 \quad \text{для всех } j \in \overline{1, q_r}, \\ d_i^{\uparrow} &= q_{i+1}, \quad d_{i+1}^{\downarrow} = q_i, \quad i = 1, 2, \dots, r-1, \end{aligned} \quad (31)$$

где

$$q_1 = 1, \quad d_1^{\downarrow} \in \begin{cases} \{1\}, & \text{если } \{\frac{r}{4}\} = 1, \\ \{1, 2, \dots, \rho - 1\}, & \text{если } \{\frac{r}{4}\} = 2, \\ \{\rho - 1\}, & \text{если } \{\frac{r}{4}\} = 3. \end{cases} \quad (32)$$

Количество реберно минимальных r -слойных графов при $\{\frac{r}{4}\} = 1, 2, 3$ вычисляется по формулам

$$|\tilde{G}_{\min}(\rho, r)| = \begin{cases} 1, & \text{если } \{\frac{r}{4}\} = 1, \\ \rho - 1, & \text{если } \{\frac{r}{4}\} = 2, \\ 1, & \text{если } \{\frac{r}{4}\} = 3, \end{cases} \quad (33)$$

$$|G_{\min}(\rho, r, k)| = \begin{cases} k - \rho + 2, & \text{если } \{\frac{r}{4}\} = 1, \\ \sum_{r=1}^{\rho-1} C_{r+k-\rho+1}^r, & \text{если } \{\frac{r}{4}\} = 2, \\ C_k^{\rho-1}, & \text{если } \{\frac{r}{4}\} = 3. \end{cases} \quad (34)$$

Доказательство. По утверждению 1 граф $\Gamma^{(r)} \in G_{\min}(\rho, r)$ может быть представлен в виде последовательного объединения одного реберно минимального $\{\frac{r}{4}\}$ -слойного графа и $\lceil \frac{r}{4} \rceil$ реберно минимальных 4-слойных графов:

$$\Gamma^{(r)} = \Gamma^{(\{\frac{r}{4}\})} \cup \Gamma_1^{(4)} \cup \dots \cup \Gamma_{\lceil \frac{r}{4} \rceil}^{(4)},$$

где

$$\Gamma^{(\{\frac{r}{4}\})} \in G_{\min}(\rho, \{\frac{r}{4}\}), \quad \Gamma_1^{(4)}, \dots, \Gamma_{\lceil \frac{r}{4} \rceil}^{(4)} \in G_{\min}(\rho, 4).$$

При $r = 1, 2, 3$ формулы (31) и (32) следуют из свойств (8), (11) и (15) графа $\Gamma^{(\{\frac{r}{4}\})}$. В частности,

$$d_{\{\frac{r}{4}\}, j}^{\uparrow} \geq \rho - 1 \text{ для всех } j \in \overline{1, q_{\{\frac{r}{4}\}}}.$$

Вместе с тем при $r > 3$ по свойству (18) графа $\Gamma_1^{(4)}$ в графе $\Gamma^{(r)}$ необходимо

$$q_{\{r/4\}+1} \leq \rho - 1.$$

Следовательно, в реберно минимальном $(4 \cdot \lceil r/4 \rceil)$ -слойном графе

$$\Gamma_1^{(4)} \cup \dots \cup \Gamma_{\lceil r/4 \rceil}^{(4)}$$

количество вершин в первом слое равно $\rho - 1$. Тогда по лемме формулы (31) справедливы при любом допустимом r .

Для обоснования формул (33) и (34) заметим, что $q_r = q_{\{r/4\}}$. Значит,

$$|\tilde{G}_{\min}(\rho, r)| = |\tilde{G}_{\min}(\rho, \{\frac{r}{4}\})|$$

и

$$|G_{\min}(\rho, r, k)| = |G_{\min}(\rho, \{\frac{r}{4}\}, k)|.$$

Остается объединить результаты утверждений 2–4.

Теорема 2 доказана. $\square$

На рис. 4 представлены реберно минимальные 9-, 10- и 11-слойные графы, являющиеся начальными участками любых реберно минимальных r -слойных графов при $\{\frac{r}{4}\} = 1, 2, 3$.

Рис. 4. Реберно минимальные 9-, 10- и 11-слойные графы

4.

При r , кратном 4 (т.е. при $\{\frac{r}{4}\} = 0$), любой реберно минимальный r -слойный граф $\Gamma^{(r)} \in G_{\min}(\rho, r)$ может быть представлен в виде последовательного объединения $t = r/4 > 0$ реберно минимальных 4-слойных графов:

$$\Gamma^{(r)} = \Gamma_1^{(4)} \cup \dots \cup \Gamma_t^{(4)}, \quad \Gamma_1^{(4)}, \dots, \Gamma_t^{(4)} \in G_{\min}(\rho, 4).$$

При этом количество вершин в первом слое графа $\Gamma_1^{(4)}$ не ограничивается значением $\rho - 1$, как в случае $\{\frac{r}{4}\} = 1, 2, 3$, а может принимать любое значение $q_1 \in \{1, 2, \dots, \rho - 1\}$. Это приводит к большому разнообразию вариантов для реберно минимальных 4-слойных графов $\Gamma_1^{(4)}, \dots, \Gamma_t^{(4)}$ и r -слойных графов при $\{\frac{r}{4}\} = 0$ в целом.

Пример 3. На рис. 5 представлены примеры двух реберно минимальных 12-слойных графов при $\rho = 4$. Видно, что при $\{\frac{r}{4}\} = 0$ существуют такие реберно минимальные r -слойные графы, что $q_i > \rho - 1$ или $d_{i,j} > \rho$ при некоторых $i = 1, 2, \dots, r$, $j = 1, 2, \dots, q_i$.

Рис. 5. Примеры реберно минимальных 12-слойных графов при $\rho = 4$

Описание множества $\{G_{\min}(\rho, r), \rho \geq 2, r \geq 1, r \equiv 0 \pmod{4}\}$ представляет собой сложную комбинаторную задачу. Отметим, что одним из способов ее решения может быть реализация переборного метода, основанного на построении согласованных цепочек выделенных 3-слойных графов с учетом результатов утверждения 5.

Автор благодарен Ф.М. Малышеву за полезное обсуждение результатов работы.

Список литературы

- [1] Федченко В.А., “Показатели рассеивания линейной среды AES-подобных алгоритмов шифрования”, *Математические вопросы криптографии*, **8:3** (2017), 109–126.
- [2] Малышев Ф.М., Трифонов 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] Холл М., *Комбинаторика*, М.: Мир, 1970, 424 с.