УДК 519.17

В.Г. СКОБЕЛЕВ

ОБ ОДНОМ СЕМЕЙСТВЕ СУПЕРПОЗИЦИЙ ПЕРЕСТАНОВОК

Исследуется семейство перестановок компонент двоичной последовательности фиксированной длины, получаемое в результате всевозможных вычеркиваний элементов из суперпозиции перестановок. Показано, что исследуемое семейство перестановок может быть использовано в качестве блока управляемых перестановок – математической модели перестановочных блочных шифров. Выделены подсемейства перестановок, для которых доля неподвижных точек стремится к нулю при неограниченном росте длины двоичной последовательности.

Введение. В последнее время большое внимание уделяется исследованию математических моделей, используемых при построении шифров [1–3]. Для блочных шифров к таким моделям относится блок управляемых перестановок [4].

В криптографии стандартный термин «подстановка» [5] применяется к инъекциям $\mathbf{f}:\mathbf{E}^n \to \mathbf{E}^m \quad (\mathbf{E}=\{0,1\}; m,n \in \mathbf{N}; m \geq n)$, а термин «перестановка» – только к биекциям $\mathbf{f}:\mathbf{E}^n \to \mathbf{E}^n$, осуществляющим фиксированную перестановку компонент вектора $\mathbf{x} \in \mathbf{E}^n$. Такой терминологии будем придерживаться в дальнейшем.

Блок управляемых перестановок [4] – это функциональная схема $S_{\mathbf{f}}$, реализующая такое отображение $\mathbf{f}:\mathbf{E}^{n+k} \to \mathbf{E}^n \quad (n,k \in \mathbf{N})$, где $\mathbf{x} \in \mathbf{E}^n$ и $\mathbf{v} \in \mathbf{E}^k$ – соответственно, информационный и управляющий вектор, что: 1) при каждом фиксированном значении $\mathbf{v}_0 \in \mathbf{E}^k$ отображение $\mathbf{g}_{\mathbf{v}_0}:\mathbf{E}^n \to \mathbf{E}^n$, определенное равенством $\mathbf{g}_{\mathbf{v}_0}(\mathbf{x}) = \mathbf{f}(\mathbf{x},\mathbf{v}_0)$ – перестановка элементов множества $\mathbf{E}^n$; 2) если $\mathbf{v}_0 \neq \mathbf{v}_1$, то $\mathbf{g}_{\mathbf{v}_0} \neq \mathbf{g}_{\mathbf{v}_1}$.

Схема $S_{\mathbf{f}}$ реализует семейство перестановок $\{\mathbf{g}_{\mathbf{v}}\}_{\mathbf{v}\in\mathbf{E}^k}$ элементов множества $\mathbf{E}^n$. Ее сложность определяется способом представления в ней семейства перестановок. Верхняя граница сложности достигается для матричного блока [4] управляемых перестановок $M_{n,k} \quad (n=2^k)$. Он состоит из дешифратора

с k входами и функциональных элементов A_i $(i = 0,1,\ldots,2^k - 1)$, каждый из которых имеет $n+1$ вход (n информационных входов, а один вход, v_i – управляющий) и n выходов. Если $v_i = 0$ $(i = 0,1,\ldots,2^k - 1)$, то элемент A_i реализует тождественное отображение $\mathbf{e}: \mathbf{E}^n \to \mathbf{E}^n$, а если $v_i = 1$ – то перестановку $\mathbf{g}_i \neq \mathbf{e}$. Управляющие входы элементов A_i $(i = 0,1,\ldots,2^k - 1)$ подсоединены к выходам дешифратора, а выходы элемента A_i $(i = 0,1,\ldots,2^k - 2)$ – к информационным входам элемента A_{i+1}. Таким образом, матричный блок $M_{n,k}$ реализует семейство перестановок

$$\{\mathbf{g}_0^{\alpha_0} \circ \mathbf{g}_1^{\alpha_1} \circ \ldots \circ \mathbf{g}_{2^k-1}^{\alpha_{2^k-1}} \mid \alpha_0, \alpha_1, \ldots . \alpha_{2^k-1} \in \mathbf{E};\ \sum_{i=0}^{2^k-1} \alpha_i = 1\} \qquad (1)$$

элементов множества $\mathbf{E}^n$, где $\circ$ – операция суперпозиции, а $\mathbf{g}^1 = \mathbf{g}$ и $\mathbf{g}^0 = \mathbf{e}$.

В работе [6] показано, что удаление в матричном блоке дешифратора приводит к блоку $\mathrm{M}_{n,m}$, который реализует семейство перестановок элементов множества $\mathbf{E}^n$, имеющее вид

$$H(\mathbf{h}_1, \ldots, \mathbf{h}_m) = \{\mathbf{h}_1^{\alpha_1} \circ \ldots \circ \mathbf{h}_m^{\alpha_m} \mid \alpha_1, \ldots . \alpha_m \in \mathbf{E}\}. \qquad (2)$$

Отличие (2) от (1) состоит в том, что (1) представляет семейство перестановок в явном виде, а (2) – в неявном виде. При этом блок $\mathrm{M}_{n,m}$ реализует 2^m-элементное семейство перестановок, используя только m порождающих элементов $\mathbf{h}_1, \ldots, \mathbf{h}_m$, реализованных в явном виде. Установим характеристики семейства (2), существенные при его использовании в качестве блока управляемых перестановок.

Основные результаты. Пусть $m, n \in \mathbf{N}$ $(1 < m \leq \lfloor 0.5n \rfloor)$, а $\pi = \{B_1, \ldots, B_m\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i| \geq 2$ $(i = 1, \ldots, m)$. Обозначим $S(B_i)$ $(i = 1, \ldots, m)$ множество всех перестановок множества $\mathbf{E}^n$, которые в векторе $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbf{E}^n$ циклически переставляют компоненты, номера которых принадлежат множеству B_i, и оставляют на месте остальные компоненты вектора $\mathbf{x}$. Положим

$$F_\pi = \{H(\mathbf{h}_1, \ldots, \mathbf{h}_m) \mid \mathbf{h}_i \in S(B_i)\ (i = 1, \ldots, m)\}. \qquad (3)$$

Теорема 1. Для любых чисел $m, n \in \mathbf{N}$ $(1 < m \leq \lfloor 0.5n \rfloor)$ и любого такого разбиения $\pi = \{B_1, \ldots, B_m\}$ множества $\mathbf{N}_n$, что $|B_i| \geq 2$ $(i = 1, \ldots, m)$ элементы каждого семейства $H(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in F_\pi$ – попарно различные перестановки множества $\mathbf{E}^n$.

Доказательство. Пусть $m,n\in\mathbf{N}\ \ (1<m\le\lfloor 0.5n\rfloor)$, а $\pi=\{B_1,\ldots,B_m\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i|\ge 2\ \ (i=1,\ldots,m)$.

Пусть $H(\mathbf{h}_1,\ldots,\mathbf{h}_m)\in F_\pi$. Если $\boldsymbol{\alpha}_i=(\alpha_1^{(i)},\ldots,\alpha_m^{(i)})\in\mathbf{E}^m\ \ (i=1,2)$ и $\boldsymbol{\alpha}_1\ne\boldsymbol{\alpha}_2$, то существует такое $j\in\mathbf{N}_m$, что $\alpha_j^{(1)}\ne\alpha_j^{(2)}$. Поэтому, либо $\mathbf{h}_j^{\alpha_j^{(1)}}=\mathbf{e}$ и $\mathbf{h}_j^{\alpha_j^{(2)}}\ne\mathbf{e}$, либо $\mathbf{h}_j^{\alpha_j^{(1)}}\ne\mathbf{e}$ и $\mathbf{h}_j^{\alpha_j^{(2)}}=\mathbf{e}$. Следовательно, если $\mathbf{x}=(x_1,\ldots,x_n)\in\mathbf{E}^n$ – такой вектор, что $\sum\limits_{i=1}^{n}x_i=1$ и $x_r=1$, где $r\in B_j$, то либо $\mathbf{h}_1^{\alpha_1^{(1)}}\circ\ldots\circ\mathbf{h}_m^{\alpha_m^{(1)}}(\mathbf{x})=\mathbf{x}$ и $\mathbf{h}_1^{\alpha_1^{(2)}}\circ\ldots\circ\mathbf{h}_m^{\alpha_m^{(2)}}(\mathbf{x})\ne\mathbf{x}$, либо $\mathbf{h}_1^{\alpha_1^{(1)}}\circ\ldots\circ\mathbf{h}_m^{\alpha_m^{(1)}}(\mathbf{x})\ne\mathbf{x}$ и $\mathbf{h}_1^{\alpha_1^{(2)}}\circ\ldots\circ\mathbf{h}_m^{\alpha_m^{(2)}}(\mathbf{x})=\mathbf{x}$, т. е. $\mathbf{h}_1^{\alpha_1^{(1)}}\circ\ldots\circ\mathbf{h}_m^{\alpha_m^{(1)}}\ne\mathbf{h}_1^{\alpha_1^{(2)}}\circ\ldots\circ\mathbf{h}_m^{\alpha_m^{(2)}}$ для любых $\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2\in\mathbf{E}^m\ \ (\boldsymbol{\alpha}_1\ne\boldsymbol{\alpha}_2)$.

Теорема доказана.

Из теоремы 1 вытекает, что любое семейство перестановок $H(\mathbf{h}_1,\ldots,\mathbf{h}_m)\in$ $\in F_\pi$ – допустимое при построении блока управляемых перестановок.

Утверждение 1. Для любых чисел $m,n\in\mathbf{N}\ \ (1<m\le\lfloor 0.5n\rfloor)$ и любого такого разбиения $\pi=\{B_1,\ldots,B_m\}$ множества $\mathbf{N}_n$, что $|B_i|\ge 2\ \ (i=1,\ldots,m)$ истинно равенство

$$|F_\pi|=\prod_{i=1}^{m}(|B_i|-1)!. \tag{4}$$

Доказательство. Из определения множества $S(B_i)\ \ (i=1,\ldots,m)$ вытекает, что

$$|S(B_i)|=(|B_i|-1)!\ \ (i=1,\ldots,m). \tag{5}$$

Из формул (3) и (5) вытекает (4).

Утверждение доказано.

Из утверждения 1 вытекают два следствия.

Следствие 1. Для любого числа $n=ml\ \ (m,l\in\mathbf{N};m\ge 2,l\ge 2)$ и любого такого разбиения $\pi=\{B_1,\ldots,B_m\}$ множества $\mathbf{N}_n$, что $|B_i|=l\ \ (i=1,\ldots,m)$ истинно равенство

$$|F_\pi\ |\ =((\ nm^{-1}-1)!)^m.$$

Следствие 2. Для любого числа $n=m^2\ \ (m\in\mathbf{N};m\ge 2)$ и любого такого разбиения $\pi=\{B_1,\ldots,B_m\}$ множества $\mathbf{N}_n$, что $|B_i|=\sqrt{n}\ \ (i=1,\ldots,m)$ истинно равенство

$$|F_\pi\ |\ =((\ \sqrt{n}-1)!)^{\sqrt{n}}.$$

Для любого разбиения $\pi = \{B_1, \ldots, B_m\}$ $(1 < m \le \lfloor 0.5n \rfloor)$ множества $\mathbf{N}_n$ множество F_π определяет класс $C(F_\pi)$ перестановочных блочных шифров. При этом семейство перестановок $H(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in F_\pi$ играет роль ключа средней длительности, либо роль секретного долговременного ключа. Из следствий 1 и 2 вытекает, что при надлежащем выборе разбиения π множества $\mathbf{N}_n$ мощность множества таких ключей является субэкспонентой от числа n.

Для любого семейства перестановок $H(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in F_\pi$ истинно равенство $\mathbf{h}_1^0 \circ \ldots \circ \mathbf{h}_m^0 = \mathbf{e}$. Для того, чтобы устранить эту ситуацию, достаточно для шифра $C(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in C(F_\pi)$, определяемого семейством $H(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in F_\pi$, обеспечить такое управление, что вектор $(\alpha_2, \ldots, \alpha_m) \in \mathbf{E}^{m-1}$ – текущий фрагмент секретного сеансового ключа, а $\alpha_1 = 1$, если $\sum_{i=2}^{m} \alpha_i = 0$ и $\alpha_1 = 0$, если $\sum_{i=2}^{m} \alpha_i \neq 0$. Таким образом, мы приходим к подмножеству

$$T_\pi = \{\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m) \mid \mathbf{h}_i \in S(B_i)\ (i = 1, \ldots, m)\}, \qquad (6)$$

множества F_π, где

$$\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m) = \{\mathbf{h}_1\} \cup \{\mathbf{h}_2^{\alpha_2} \circ \ldots \circ \mathbf{h}_m^{\alpha_m} \mid \alpha_2, \ldots . \alpha_m \in \mathbf{E},\ \sum_{i=2}^{m} \alpha_i \ge 1\}. \qquad (7)$$

Вектор $\mathbf{x} \in \mathbf{E}^n$ назовем неподвижной точкой семейства перестановок $\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in T_\pi$, если $\mathbf{h}_1(\mathbf{x}) = \mathbf{x}$ или существуют такие $\alpha_2, \ldots . \alpha_m \in \mathbf{E}$ $\left(\sum_{i=2}^{m} \alpha_i \ge 1\right)$, что $\mathbf{h}_2^{\alpha_2} \circ \ldots \circ \mathbf{h}_m^{\alpha_m}(\mathbf{x}) = \mathbf{x}$. Обозначим $S_{fxd}(\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m))$ множество всех неподвижных точек семейства перестановок $\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in T_\pi$.

Теорема 2. Пусть $n = \sum_{i=1}^{m} p_i$, где p_i $(i = 1, \ldots, m)$ – простые числа, а $\pi = \{B_1, \ldots, B_m\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i| = p_i$ $(i = 1, \ldots, m)$. Тогда для каждого семейства перестановок $\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m) \in T_\pi$ истинно равенство

$$|S_{fxd}(\tilde{H}(\mathbf{h}_1, \ldots, \mathbf{h}_m))| = |\mathbf{E}^n| \left(1 - \prod_{i=1}^{m} (1 - 2^{1-p_i})\right). \qquad (8)$$

Доказательство. Так как p_i $(i = 1, \ldots, m)$ – простое число, то вектор $\mathbf{x} \in \mathbf{E}^n$ не является неподвижной точкой перестановки $\mathbf{h}_i$ тогда и только тогда, когда

его компоненты, номера которых принадлежат множеству B_i, принимают как значение 0, так и значение 1.

Циклы, определяемые перестановками $\mathbf{h}_1,\ldots,\mathbf{h}_m$, попарно не пересекаются, а объединение множеств входящих в эти циклы элементов совпадает с $\mathbf{N}_n$.

Следовательно, вектор $\mathbf{x}\in\mathbf{E}^n$ не является неподвижной точкой ни для перестановки $\mathbf{h}_1$, а также ни для одной из перестановок $\mathbf{h}_2^{\alpha_2}\circ\ldots\circ\mathbf{h}_m^{\alpha_m}$ $\left(\alpha_2,\ldots.\alpha_m\in\mathbf{E},\ \sum_{i=2}^{m}\alpha_i\geq 1\right)$ тогда и только тогда, когда для всех $i=1,\ldots,m$ компоненты вектора $\mathbf{x}$, номера которых принадлежат множеству B_i, принимают как значение 0, так и значение 1. Отсюда вытекает, что

$$|S_{fxd}(\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_m))| = |\mathbf{E}^n|-\prod_{i=1}^{m}(2^{p_i}-2) = |\mathbf{E}^n|-\prod_{i=1}^{m}2^{p_i}(1-2^{1-p_i}) =$$

$$= |\mathbf{E}^n|-\left(\prod_{i=1}^{m}2^{p_i}\right)\left(\prod_{i=1}^{m}(1-2^{1-p_i})\right) = |\mathbf{E}^n|-|\mathbf{E}^n|\prod_{i=1}^{m}(1-2^{1-p_i}) =$$

$$= |\mathbf{E}^n|\left(1-\prod_{i=1}^{m}(1-2^{1-p_i})\right).$$

Теорема доказана.

Следствие 3. Пусть $n=\sum_{i=1}^{m}p_i$, где p_i $(i=1,\ldots,m)$ – простые числа, а $\pi=\{B_1,\ldots,B_m\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i|=p_i$ $(i=1,\ldots,m)$. Если $p_i\to\infty$ для всех значений $i\in\mathbf{N}_m$, то для каждого семейства перестановок $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_m)\in T_\pi$ почти все $\mathbf{x}\in\mathbf{E}^n$ не являются неподвижными точками.

Доказательство. Из равенства (8) вытекает, что для каждого семейства перестановок $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_m)\in T_\pi$ доля ν_{fxd} векторов $\mathbf{x}\in S_{fxd}(\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_m))$ определяется равенством

$$\nu_{fxd} = 1-\prod_{i=1}^{m}(1-2^{1-p_i}).$$

Если $p_i\to\infty$ для всех значений $i\in\mathbf{N}_m$, то $\nu_{fxd}\to 0$.

Следствие доказано.

Заключение. В работе исследованы свойства множества F_π представленных в неявном виде семейств суперпозиций перестановок компонент вектора $\mathbf{x}\in\mathbf{E}^n$. Показано, что его подмножество T_π может быть использовано в качестве блока управляемых перестановок – математической модели перестановочных блочных шифров.

Анализ свойств множеств F_π и T_π, характеризуемых в терминах решетки разбиений множества $\mathbf{N}_n$ – возможное направление исследований. Другое направление состоит в обобщении полученных результатов на множества семейств суперпозиций перестановок компонент вектора $\mathbf{x} \in \mathbf{E}^n$, определяемые в терминах покрытий множества $\mathbf{N}_n$.

В.Г. Скобелєв

ПРО ОДНУ СІМ'Ю СУПЕРПОЗИЦІЙ ПЕРЕСТАВЛЕНЬ

Досліджено сім'ю переставлень компонент бінарної послідовності, що має фіксовану довжину, яку може бути отримано внаслідок найрізноманітніших викреслювань елементів фіксованої суперпозиції переставлень. Встановлено, що досліджувану сім'ю переставлень може бути використано як блок керуючих переставлень – математичної моделі блокових шифрів, які базуються на переставленнях. Виділено підсім'ї переставлень для яких частка нерухомих точок прямує до нуля за умови, що довжина бінарної послідовності необмежено зростає.

V.G. Skobelev

ON A FAMILY OF SUPERPOSITIONS OF PERMUTATIONS

A family of permutations of binary sequences of fixed length, such that a family can be generated as a result of various element deletions in a fixed superposition of permutations, is analyzed. It is established that this family can be applied as a block of controllable permutations, i.e., as a mathematical model of transpositions of block ciphers. Sub-families are chosen, such that a part of fixed points converges to zero if the length of binary sequence grows unlimitedly.

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С. и др.* Основы криптографии. – М.: Гелиос АРВ, 2002. – 480 с.
2. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. − М.: ТРИУМФ, 2003. − 816 с.
3. *Харин Ю.С., Берник В.И., Матвеев Г.В. и др.* Математические и компьютерные основы криптологии. − Минск: Новое знание, 2003. − 382 с.
4. *Молдовян А.А., Молдовян Н.А., Гуц Н.Д. и др.* Криптография. Скоростные шифры. – СПб: БХВ-Петербург, 2002. – 496 с.
5. *Сачков В.Н.* Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.
6. *Скобелев В.В., Скобелев В.Г.* Анализ шифрсистем. – Донецк: ИПММ НАН Украины, 2009. – 479 с.

Получено 07.07.2010

Об авторе:

Скобелев Владимир Геннадиевич,
доктор технических наук, профессор, ведущий научный сотрудник
отдела теории управляющих систем
Института прикладной математики и механики НАН Украины, г. Донецк.
e-mail: skbv@iamm.ac.donetsk.ua