# ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.7 DOI 10.17223/20710410/60/1

## ХАРАКТЕРИЗАЦИЯ БИЕКТИВНЫХ APN-ОТОБРАЖЕНИЙ В ТЕРМИНАХ РАССТОЯНИЯ МЕЖДУ ПОДГРУППАМИ СИММЕТРИЧЕСКОЙ ГРУППЫ

А. Р. Белов

*Ярославский государственный университет им. П. Г. Демидова, г. Ярославль, Россия*

**E-mail:** ashmedey@gmail.com

Изучаются биективные APN-отображения, заданные на конечном поле чётной характеристики. Свойство биективного отображения быть APN-отображением выражается в терминах расстояния Хэмминга между подгруппами симметрической группы. Предложен новый подход к построению биективных APN-отображений: задача построения APN-перестановки сведена к поиску подгруппы симметрической группы, которая далека (в смысле расстояния Хэмминга) от группы сдвигов конечного поля $\mathbb{F}_{2^n}$, и решению системы уравнений сопряжения.

**Ключевые слова:** *APN-отображение, перестановка, симметрическая группа, расстояние Хэмминга.*

## CHARACTERIZATION OF APN-PERMUTATIONS IN TERMS OF HAMMING DISTANCE BETWEEN SUBGROUPS OF SYMMETRIC GROUP

A. R. Belov

*P. G. Demidov Yaroslavl State University, Yaroslavl, Russia*

In the paper, we give a characterization of APN-permutations in terms of the Hamming distance between subgroups of the symmetric group. Let

$$T = \{\tau_\alpha \in S(\mathbb{F}_{2^n}) : \alpha \in \mathbb{F}_{2^n} \ \& \ \forall x \in \mathbb{F}_{2^n} \ (\tau_\alpha(x) = x + \alpha)\}.$$

Then permutation $\pi \in S(\mathbb{F}_{2^n})$ is APN if and only if $\mathrm{d}(T, T') = 2^n - 2$, where $T' = \pi^{-1} \cdot T \cdot \pi$ and $\mathrm{d}(T, T')$ is the Hamming distance between subgroups $T, T' \leqslant S(\mathbb{F}_{2^n})$. Using this characterization, a new approach to the construction of APN-permutations is proposed: the problem of constructing an APN-permutation is reduced to finding a suitable group $T'$ and solving the simultaneous conjugation problem $T = x^{-1} \cdot T' \cdot x$. To find suitable groups $T'$, a combinatorial approach is used, which consists in constructing some graph $G(T)$ associated with the group $T$ and searching in that graph for a maximum independent sets. Let $T' = \langle \tau_1, \tau_2, \ldots, \tau_n \rangle$. Then $\mathrm{d}(\langle \tau_i \rangle, T) = 2^n - 2$ if and only if a set of transpositions in decomposition of $\tau_i$ is a maximum independent set in $G(T)$. We have listed all maximum independent sets in the graph $G(T)$ associated with the translation group $T$ of the field $\mathbb{F}_{2^4}$. In this case the group $T'$ cannot be

constructed. Thus we have obtained the well-known result about the non-existence of APN permutations in $\mathbb{F}_{2^4}$. APN-permutations in the field $\mathbb{F}_{2^3}$ are classified by listing all possible candidates for the group $T'$: there are 8 possible groups.

**Keywords:** *APN mapping, permutation, symmetric group, Hamming distance, simultaneous conjugacy.*

## Введение

Одной из характеристик нелинейных элементов блочных шифров, которая обеспечивает устойчивость к некоторым методам анализа, является *дифференциальная равномерность* [1]. Отображения, обладающие оптимальной дифференциальной равномерностью, называются *почти совершенно нелинейными отображениями* или *APN-отображениями*.

**Определение 1.** Отображение

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

называется *APN-отображением*, если для всех $a \in \mathbb{F}_{2^n}^*$ и $b \in \mathbb{F}_{2^n}$ уравнение

$$f(x + a) - f(x) = b$$

имеет не более двух решений.

Проблема существования биективных APN-отображений на сегодняшний день не решена. Известно, что для полей $\mathbb{F}_{2^n}$, где $n = 2, 4$, таких отображений не существует [2]. Первым примером APN-перестановки для полей чётной размерности была перестановка, построенная в работе [3] для $n = 6$. Для других чётных значений $n > 6$ вопрос остаётся открытым.

Для характеризации APN-свойства будем использовать понятие *расстояния Хэмминга между перестановками*. Пусть $\Omega$ — конечное множество из $n$ элементов, $S(\Omega)$ — симметрическая группа на $\Omega$.

**Определение 2.** *Расстоянием Хэмминга между перестановками* $f, g \in S(\Omega)$ называется

$$\mathrm{d}(f, g) = |\{x \in \Omega : f(x) \neq g(x)\}|.$$

**Определение 3.** *Расстоянием Хэмминга между подгруппами* $G, G' < S(\Omega)$ называется

$$\mathrm{d}(G, G') = \min_{\substack{g \in G \setminus \{e\} \\ g' \in G' \setminus \{e\}}} \mathrm{d}(g, g').$$

**Утверждение 1.** Пусть разложение перестановок $f, g \in S(\Omega)$ в произведение независимых циклов имеет вид

$$f = \omega_1 \dots \omega_s \tau_1 \dots \tau_k, \quad g = \omega_1 \dots \omega_s \sigma_1 \dots \sigma_l,$$

где $\tau_i, \omega_i, \sigma_i$ — транспозиции и $\tau_i \neq \sigma_j$ для всех $i, j$. Тогда

$$\mathrm{d}(f, g) = n - 2s - |\mathrm{fix}(f) \cap \mathrm{fix}(g)|,$$

где $\mathrm{fix}(\pi) = \{x \in \Omega : \pi(x) = x\}$.

## 1. Характеризация биективных APN-отображений

Любой элемент поля $\alpha \in \mathbb{F}_{2^n}$ определяет биективное отображение

$$\tau_\alpha : \mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}, \quad x \longmapsto x + \alpha.$$

Множество всех таких отображений $T = \{\tau_\alpha : \alpha \in \mathbb{F}_{2^n}\}$ образует подгруппу симметрической группы $S(\mathbb{F}_{2^n})$. Отметим простейшие свойства группы $T$:

1) $T$ состоит из перестановок порядка 2;
2) каждая перестановка $\tau \in T \setminus \{e\}$ не имеет неподвижных точек;
3) каждая перестановка $\tau \in T \setminus \{e\}$ раскладывается в произведение независимых циклов следующим образом:

$$\tau = (\alpha_1\alpha_2)(\alpha_3\alpha_4)\dots(\alpha_{2^n-1}\alpha_{2^n}),$$

где $\alpha_i$, $i = 1, \dots, 2^n$ — различные элементы поля $\mathbb{F}_{2^n}$;
4) группа $T$ изоморфна прямому произведению $n$ циклических групп порядка 2.

Если $\{e_1, e_2, \dots, e_n\}$ — некоторый базис $\mathbb{F}_{2^n}$ над $\mathbb{F}_2$, то в качестве образующих группы $T$ можно взять перестановки $\tau_{e_1}, \tau_{e_2}, \dots, \tau_{e_n}$.

Свойство биективного отображения $f$ быть APN-отображением можно выразить через метрические отношения между элементами сопряжённых групп.

**Утверждение 2.** Перестановка $f \in S(\mathbb{F}_{2^n})$ является APN-отображением тогда и только тогда, когда

$$\mathrm{d}(T, T') = 2^n - 2,$$

где $T' = f^{-1} \cdot T \cdot f$.

***Доказательство.*** Пусть $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ — биективное APN-отображение. Тогда по определению уравнение

$$f(x + a) - f(x) = b$$

имеет не более двух решений для всех $a \in \mathbb{F}_{2^n}^*$ и $b \in \mathbb{F}_{2^n}$. Это уравнение можно переписать в виде

$$f(x + a) = f(x) + b.$$

Если посмотреть на $f$ как на элемент группы $S(\mathbb{F}_{2^n})$, то в этом уравнении слева стоит произведение перестановок $\tau_a$ и $f$, а справа — произведение $f$ и $\tau_b$. С учётом этого уравнение можно записать в виде

$$[\tau_a \cdot f](x) = [f \cdot \tau_b](x), \tag{1}$$

где через $f \cdot g$ обозначается произведение перестановок $f$ и $g$ [4], определённое по правилу $[f \cdot g](x) = g(f(x))$. Домножив обе части уравнения (1) слева на $f^{-1}$, получим

$$[f^{-1} \cdot \tau_a \cdot f](x) = \tau_b(x).$$

При таком преобразовании число решений не изменилось.

Введём обозначение $\tau'_a = f^{-1} \cdot \tau_a \cdot f$. Тогда уравнение примет окончательный вид

$$\tau'_a(x) = \tau_b(x), \tag{2}$$

где в левой части на $x$ действует перестановка из $T'$, а в правой — один из сдвигов группы $T$. Пусть $m_{a,b}$ — число решений уравнения (2). Тогда

$$m_{a,b} = 2^n - \mathrm{d}(\tau'_a, \tau_b).$$

Так как по условию $m_{a,b} \leqslant 2$, то $\mathrm{d}(\tau'_a, \tau_b) \geqslant 2^n - 2$. Неравенство верно для всех $\tau'_a \in \in T' \setminus \{e\}$ и $\tau_b \in T \setminus \{e\}$, а значит, $\mathrm{d}(T, T') \geqslant 2^n - 2$.

Так как перестановки $\tau'_a$ и $\tau_b$ сопряжены, они имеют одинаковую цикловую структуру. Выпишем разложение в произведение независимых циклов перестановки $\tau'_a$ и всех перестановок группы $T$:

$$\begin{aligned}
\tau'_a &= \sigma_1 \dots \sigma_{2^n}, \\
\tau_1 &= e, \\
\tau_2 &= \pi_{1,2} \dots \pi_{2^{n-1},2}, \\
&\dots \\
\tau_{2^n} &= \pi_{1,2^n} \dots \pi_{2^{n-1},2^n}.
\end{aligned}$$

Все транспозиции $\pi_{i,j}$ различны. Их количество равно $(2^n-1)2^{n-1}$, что совпадает с числом всевозможных транспозиций, составленных из $2^n$ элементов поля $\mathbb{F}_{2^n}$. Значит, для любой транспозиции $\sigma_i$ из разложения $\tau'_a$ найдётся элемент $\tau_j$, для которого $\sigma_i = \pi_{s,j}$. Кроме того, $\sigma_i$ — единственная транспозиция из разложения $\tau'_a$, которая встречается в разложении $\tau_j$. Поэтому, используя утверждение 1, получаем

$$d(\tau'_a, \tau_j) = 2^n - 2 \cdot 1 - 0 = 2^n - 2.$$

Значит, $\mathrm{d}(T, T') = 2^n - 2$.

Обратно, пусть $\mathrm{d}(T, T') = 2^n - 2$. Если предположить, что $f$ не является APN-перестановкой, то получим для некоторых $\tau'_a \in T' \setminus \{e\}$ и $\tau_b \in T \setminus \{e\}$ расстояние

$$\mathrm{d}(\tau'_a, \tau_b) = 2^n - m_{a,b} < 2^n - 2,$$

что противоречит условию $\mathrm{d}(T, T') = 2^n - 2$. ■

## 2. Комбинаторный подход к построению APN-перестановок

Используя полученную характеризацию, можно предложить следующий подход к построению APN-перестановок:

1) Найти подгруппу $T' \leqslant S(\mathbb{F}_{2^n})$, изоморфную группе сдвигов $T$, для которой $\mathrm{d}(T, T') = 2^n - 2$. Эта подгруппа должна удовлетворять свойствам 1–4 группы $T$.
2) Найти такую сопрягающую перестановку $f \in S(\mathbb{F}_{2^n})$, что $T' = f^{-1} \cdot T \cdot f$.
   Для этого нужно решить систему уравнений сопряжения. Достаточно искать сопрягающую перестановку, которая переводит образующие одной группы в образующие другой группы. Таким образом, система состоит из $n$ уравнений сопряжения.

Основная сложность здесь заключается в поиске подходящей группы $T'$. Для решения второй задачи можно воспользоваться одним из алгоритмов решения подобных систем [5–7].

**Пример 1.** Пусть $n = 3$ и поле $\mathbb{F}_{2^3}$ задано корнем $\alpha$ полинома $x^3 + x + 1$. Тогда если каждому элементу поля $a_0 + a_1\alpha + a_2\alpha^2$ поставить в соответствие целое число $a_0 + a_1 2 + a_2 2^2$, то группа $T$ состоит из следующих элементов:

$$\begin{gathered}
\tau_0 = e; \\
\tau_1 = (01)(23)(45)(67);\ \tau_2 = (02)(13)(46)(57); \\
\tau_3 = (03)(12)(47)(56);\ \tau_4 = (04)(15)(26)(37); \\
\tau_5 = (05)(14)(27)(36);\ \tau_6 = (06)(17)(24)(35); \\
\tau_7 = (07)(16)(25)(34).
\end{gathered}$$

В качестве $T'$ возьмём группу из следующих элементов:

$$\tau'_0 = e;$$
$$\tau'_1 = (01)(27)(34)(56);\ \tau'_2 = (07)(12)(35)(46);$$
$$\tau'_3 = (02)(17)(36)(45);\ \tau'_4 = (03)(14)(26)(57);$$
$$\tau'_5 = (04)(13)(25)(67);\ \tau'_6 = (05)(16)(24)(37);$$
$$\tau'_7 = (06)(15)(23)(47).$$

Для неё $\mathrm{d}(T, T') = 2^3 - 2 = 6$. Если мы найдём отображение, которое сопряжением переводит $T$ в $T'$, то оно будет искомым биективным APN-отображением. Для этого достаточно найти отображение, которое переводит множество порождающих перестановок группы $T$ в множество порождающих группы $T'$, т. е. решить уравнение

$$x^{-1} \cdot \{\tau_1, \tau_2, \tau_4\} \cdot x = \{\tau'_1, \tau'_2, \tau'_6\}.$$

Допустим, что искомая перестановка $f$ переводит $\tau_1$ в $\tau'_1$, $\tau_2$ в $\tau'_2$, $\tau_4$ в $\tau'_6$ и $f(0) = 0$. Тогда транспозиция $(01)$ должна переходить в $(01)$, $(02)$ — в $(07)$, а транспозиция $(04)$ — в $(05)$. Отсюда $f(1) = 1$, $f(2) = 7$, $f(4) = 5$. Используя эти данные, получаем, что $(23)$ должна переходить в $(27)$, $(45)$ — в $(56)$, $(46)$ — в $(35)$. Значит, $f(3) = 2$, $f(5) = 6$, $f(6) = 3$. Наконец, транспозиция $(67)$ должна переходить в $(34)$, откуда $f(7) = 4$. Искомая перестановка равна

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 7 & 2 & 5 & 6 & 3 & 4 \end{pmatrix}.$$

В примере 1 для построения группы $T'$ использована известная APN-перестановка:

$$T' = \mathrm{inv}^{-1} \cdot T \cdot \mathrm{inv},$$

где $\mathrm{inv} = (2,5)(3,6)(4,7)$ — перестановка обращения в поле $\mathbb{F}_{2^3}$. Но как построить $T'$ без использования известных APN-перестановок?

Можно попытаться построить группу $T'$, используя следующую стратегию:

1) найти инволюцию $\tau' \in S(\mathbb{F}_{2^n})$ без неподвижных точек с условием $\mathrm{d}(T, \langle \tau' \rangle) = 2^n - 2$;
2) достроить $\langle \tau' \rangle$ до группы $\langle \tau', \tau'_2, \tau'_3, \ldots, \tau'_n \rangle$, изоморфной $T$ и находящейся на расстоянии $2^n - 2$ от неё.

Переведём первую подзадачу на язык теории графов. Определим граф $G = (V, E)$ следующим образом: $V$ — множество всевозможных транспозиций из $S(\mathbb{F}_{2^n})$; $(v_1, v_2) \in E \iff v_1$ и $v_2$ зависимы или $v_1$ и $v_2$ входят в разложение некоторого сдвига $\tau \in T$.

**Пример 2.** Для группы сдвигов из примера 1 часть графа $G$, соответствующая сдвигам $\tau_1, \tau_3, \tau_5$, приведена на рис. 1. Рёбра чёрного цвета обусловлены вхождением транспозиций в разложение сдвигов $\tau_1, \tau_3, \tau_5$, а цветные рёбра — зависимостью транспозиций.

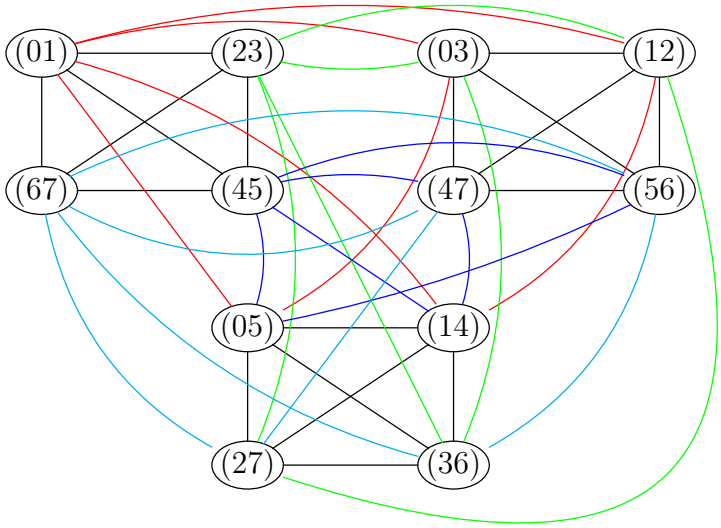


Рис. 1

**Утверждение 3.** Пусть $\tau' = \omega_1 \dots \omega_{2^{n-1}} \in S(\mathbb{F}_2^n)$ — инволюция без неподвижных точек; $\omega_i$ — независимые транспозиции ($i = 1, \dots, 2^{n-1}$). Тогда условие $\mathrm{d}(\langle \tau' \rangle, T) = 2^n - 2$ выполнено тогда и только тогда, когда множество вершин $\{\omega_1, \dots, \omega_{2^{n-1}}\}$ является наибольшим независимым множеством в графе $G$.

***Доказательство.*** Следует из определения графа $G$ и утверждения 1. ■

Для построения всех подходящих инволюций можно воспользоваться алгоритмом перечисления максимальных независимых подмножеств, среди которых нужно выбрать наибольшие. В работе [8] предложен алгоритм решения этой задачи, имеющий сложность $O(ve\mu)$, где $v, e, \mu$ — число вершин, рёбер и максимальных независимых множеств в графе соответственно. В данном случае граф $G$ имеет $v = (2^n - 1)2^{n-1}$ вершин и является $d$-регулярным, где $d = (2^{n-1} - 1) + 2(2^n - 2)$. Поэтому число вершин равно $e = vd/2 = 5 \cdot 2^{n-3}(2^n - 2)(2^n - 1)$. Параметр $\mu$ можно грубо оценить сверху количеством независимых множеств $i(G)$ в графе $G$. В работе [9] дана оценка на $i(G)$ для $d$-регулярных графов:

$$i(G) \leqslant (2^{d+1} - 1)^{v/2d}.$$

Перечисление всех возможных инволюций возможно лишь при значениях $n < 5$. Так, для $n = 4$ число максимальных независимых множеств в графе равно $\mu = 1390080$, среди которых имеется 167040 наибольших.

Пусть инволюция $\tau'$ уже построена. Достроим её до группы $\langle \tau', \tau'_2, \dots, \tau'_n \rangle \cong T$. Образующие этой группы следует искать среди инволюций без неподвижных точек $g$, для которых выполнены следующие два условия:

1) $g$ коммутирует с $\tau'$, т. е. $g\,\tau' g^{-1} = \tau'$;
2) разложение $g$ в произведение независимых циклов образует наибольшее независимое множество в графе $G$.

Подсчитаем количество всевозможных инволюций $g$, для которых выполнено первое условие. Обозначим множество таких $g$ через $C(\tau')$. Пусть разложение $\tau'$ имеет вид

$$\tau' = (a_1, b_1) \dots (a_{2^{n-1}}, b_{2^{n-1}}).$$

Тогда из условия 1 следует

$$g\,\tau' g^{-1} = (g(a_1), g(b_1)) \dots (g(a_{2^{n-1}}), g(b_{2^{n-1}})) = \tau',$$

т. е. $g$ перемешивает циклы $\tau'$: для любой транспозиции $(a_i, b_i)$ найдётся другая транспозиция $(a_j, b_j)$, такая, что $g(a_i) = a_j$, $g(b_i) = b_j$ или $g(a_i) = b_j$, $g(b_i) = a_j$. Таким образом, для построения всевозможных инволюций $g$ достаточно $\mathrm{C}^2_{2^{n-1}}\mathrm{C}^2_{2^{n-1}-2}\dots\mathrm{C}^2_2$ способами разбить на пары транспозиции из разложения $\tau'$, а затем для каждого варианта $2^{n-2}$ способами выбрать значения $g(a_i), g(b_i), 1 \leqslant i \leqslant 2^{n-1}$. Получаем

$$|C(\tau')| = 2^{n-2}\mathrm{C}^2_{2^{n-1}}\mathrm{C}^2_{2^{n-1}-2}\dots\mathrm{C}^2_2.$$

Среди всех $g \in C(\tau')$ нужно оставить только те, которые удовлетворяют условию 2. Обозначим множество таких инволюций через $MC(\tau')$. Для построения группы $T'$ осталось выбрать $n-1$ образующих $\tau'_2, \dots, \tau'_n \in MC(\tau')$. Такой способ построения группы $T'$ возможен для небольших значений $n \leqslant 5$.

Приведём результаты вычислительных экспериментов для $n = 3, 4$. В случае $n = 3$ граф $G$ имеет 56 наибольших независимых множеств. Каждому независимому множеству соответствует инволюция $\tau'$, для которой $|C(\tau')| = 12$, $|MC(\tau')| = 6$. По каждому множеству $MC(\tau')$ восстанавливается группа $T'$. Таким образом получены все восемь групп, удовлетворяющих условиям утверждения 2:

$$\begin{aligned}
T_1 &= \langle (01)(25)(37)(46),\ (02)(15)(36)(47),\ (06)(14)(23)(57)\rangle;\\
T_2 &= \langle (01)(27)(35)(46),\ (06)(14)(25)(37),\ (07)(12)(36)(45)\rangle;\\
T_3 &= \langle (01)(26)(34)(57),\ (02)(16)(35)(47),\ (07)(15)(24)(36)\rangle;\\
T_4 &= \langle (01)(24)(36)(57),\ (06)(13)(25)(47),\ (07)(15)(23)(46)\rangle;\\
T_5 &= \langle (01)(26)(35)(47),\ (02)(16)(37)(45),\ (07)(14)(23)(56)\rangle;\\
T_6 &= \langle (01)(25)(36)(47),\ (03)(16)(24)(57),\ (07)(14)(26)(35)\rangle;\\
T_7 &= \langle (01)(24)(37)(56),\ (03)(17)(25)(46),\ (06)(15)(27)(34)\rangle;\\
T_8 &= \langle (01)(27)(34)(56),\ (06)(15)(23)(47),\ (07)(12)(35)(46)\rangle.
\end{aligned}$$

Среди $8! = 40320$ перестановок имеется 10752 APN-перестановок, которые разбиваются на восемь классов эквивалентности: каждая APN-перестановка является решением одной из восьми систем уравнений сопряжения $T_i = x^{-1} \cdot T \cdot x$. Для $n = 4$ граф $G$ имеет 167040 наибольших независимых множеств. При этом для каждого независимого множества и соответствующей инволюции $\tau'$ выполняется $|C(\tau')| = 1680$, $|MC(\tau')| = 0$, что соответствует известному результату [2] о несуществовании APN-перестановок для $n = 4$.

## Заключение

В работе представлен способ характеризации биективных APN-отображений с помощью метрических отношений между элементами сопряжённых групп. Предложен подход к построению биективных APN-отображений: задача сведена к поиску группы $T'$ специального вида и решению уравнения сопряжения $T' = x^{-1} \cdot T \cdot x$, где $T$ — группа сдвигов поля $\mathbb{F}_{2^n}$. Целью дальнейших исследований в этом направлении является изучение задачи эффективного построения группы $T'$.

## ЛИТЕРАТУРА


1. *Городилова А. А.* От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3 (33). С. 16–44.
2. *Hou X.-D.* Affinity of permutations of $F_2^n$ // Discr. Appl. Math. Special Issue: Coding and Cryptography Archive. 2006. V. 154. P. 313–325.
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An apn permutation in dimension six // Amer. Math. Soc. 2010. No. 518. P. 33–42.
4. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра: Учебник. 2-е изд., испр. и доп. СПб.: Лань, 2015. 608 с.
5. *Fontet M.* Calcul de Centralisateur d'un Grupe de Permutatations // Bull. Soc. Math. France Mem. 1977. No. 49–50. P. 53–63.
6. *Sridhar M. A.* A fast algorithm for testing isomorphism of permutation networks // IEEE Trans. Computers. 1989. No. 38 (6). P. 903–909.
7. *Brodnik A., Malnič A., and Požar R.* The Simultaneous Conjugacy Problem in the Symmetric Group. `https://arxiv.org/abs/1907.07889`. 2020.
8. *Tsukiyama S., Ide M., Ariyoshi H., and Shirakawa I.* A new algorithm for generating all the maximal independent sets // SIAM J. Comput. 1977. No. 6. P. 505–517.
9. *Zhao Y.* The number of independent sets in a regular graph // Combinatorics, Probability and Computing. 2010. V. 19. P. 315–320.


## REFERENCES


1. *Gorodilova A. A.* Ot kriptoanaliza shifra k kriptograficheskomu svoystvu bulevoy funktsii [From cryptanalysis to cryptographic property of a Boolean function]. Prikladnaya Diskretnaya Matematika, 2016, no. 3 (33), pp. 16–44. (in Russian)
2. *Hou X.-D.* Affinity of permutations of $F_2^n$. Discr. Appl. Math. Special Issue: Coding and Cryptography Archive, 2006, vol. 154, pp. 313–325.
3. *McQuistan M. T., Wolfe A. J., Browning K. A., and Dillon J. F.* An apn permutation in dimension six. Amer. Math. Soc., 2010, no. 518, pp. 33–42.
4. *Glukhov M. M., Elizarov V. P., and Nechaev A. A.* Algebra: Uchebnik [Algebra: Textbook]. Saint Petersburg, Lan Publ., 2015. 608 p. (in Russian)
5. *Fontet M.* Calcul de Centralisateur d'un Grupe de Permutatations. Bull. Soc. Math. France Mem., 1977, no. 49–50, pp. 53–63.
6. *Sridhar M. A.* A fast algorithm for testing isomorphism of permutation networks. IEEE Trans. Computers, 1989, no. 38 (6), pp. 903–909.
7. *Brodnik A., Malnič A., and Požar R.* The Simultaneous Conjugacy Problem in the Symmetric Group. `https://arxiv.org/abs/1907.07889`, 2020.
8. *Tsukiyama S., Ide M., Ariyoshi H., and Shirakawa I.* A new algorithm for generating all the maximal independent sets. SIAM J. Comput., 1977, no. 6, pp. 505–517.
9. *Zhao Y.* The number of independent sets in a regular graph. Combinatorics, Probability and Computing, 2010, vol. 19, pp. 315–320.