МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2020 Т. 11 № 3 С. 121–138

УДК 519.719.2 DOI https://doi.org/10.4213/mvk335

Построение подстановок пространства V_{2m} с использованием $(2m, m)$-функций

Д. Б. Фомин

Национальный исследовательский университет «Высшая школа экономики», Москва

Получено 6.VII.2020

Аннотация. Способ построения подстановок, основанный на конструкции типа «бабочка», обобщается на случай произвольного арифметического векторного пространства четной размерности над полем из двух элементов. Предложены подходы к построению подстановок с использованием неравновероятных $(2m, m)$-функций с высокой нелинейностью.

Ключевые слова: подстановка, векторная булева функция, нелинейность

Construction of permutations on the space V_{2m} by means of $(2m, m)$-functions

D. B. Fomin

National Research University Higher School of Economics, Moscow

Abstract. We generalize the method of construction of permutations based on the Butterfly structure for the case of arbitrary arithmetic space with even dimension over the field of two elements. An approach to the construction of permutations by means of nonbalanced $(2m, m)$-functions with high nonlinearity is suggested.

Keywords: substitution, vectorial Boolean function, nonlinearity

Citation: Matematicheskie Voprosy Kriptografii, 2020, v. 11, № 3, pp. 121–138 (Russian)

Введение

Подстановки являются составной частью таких современных криптографических примитивов, как блочные шифры, хэш-функции и некоторые поточные шифры. В последние годы появляются все новые способы построения подстановок с низкой дифференциальной равномерностью, высокой алгебраической степенью нелинейности и высокой нелинейностью [1–5]. Большая часть этих работ посвящена способам построения новых классов подстановок на основе имеющихся, в частности с использованием подстановок меньшей размерности. Стоит отметить подходы, связанные с построением подстановок на основе сетей Фейстеля [6–8], сетей типа Mysty [6, 9, 10], на основе SPN сетей [11–13], а также некоторые другие [3, 14, 15].

В настоящей работе исследуется подход к построению подстановок на основе так называемого TU-представления [15, 16], в некотором смысле обобщающего сети Фейстеля. Подстановки, построенные по этому принципу, далее будут называться F-конструкциями (Feistel-like constructions). TU-представление, как правило, используется при исследовании декомпозиции подстановок [15–17]. Здесь же решается обратная задача — построение подстановок с гарантированными криптографическими характеристиками. Данная работа обобщает результаты [5] и содержит обоснование полученных в ней экспериментальных результатов.

В разделе 1 в общем виде описана F-конструкция и введены основные обозначения и определения. В разделе 2 описан способ задания $(2m, m)$-функций, основанный на построении сбалансированных функций из несбалансированных, имеющих высокую нелинейность. Такой подход аналогичен подходу, изложенному в [18], однако он изложен с более общих позиций. В разделе 3 рассмотрен способ построения подстановок с использованием F-конструкции и результатов раздела 2. В разделе 4 предложен алгоритм поиска подстановок, заключающийся в последовательном поиске функций специального вида.

1. Основные понятия

Полем из двух элементов будем называть множество $\mathbb{F}_2 = \{0, 1\}$ с заданными естественным образом операциями сложения $+$ и умножения $\cdot$. Пусть $(V_n, +) = \left\{(a_0, a_1, \ldots, a_{n-1}), a_i \in \mathbb{F}_2, i \in \overline{0, n-1}\right\}$ — арифметическое векторное пространство размерности n, $\theta = (0, 0, \ldots, 0)$ — нуль векторного пространства. Если рассмотреть аддитивную группу

векторного пространства $(V_n, \oplus)$ и задать специальным образом операцию умножения, то можно построить поле, которое будем обозначать $(\mathbb{F}_{2^n}, +, \cdot)$.

Для $a \in V_n$, $b \in V_m$ через $a\|b \in V_{n+m}$ обозначим конкатенацию двух векторов.

Для произвольных $a, b \in V_n$ скалярным произведением векторов называется элемент поля $\mathbb{F}_2$, определяемый формулой

$$\langle a, b\rangle = \sum_{i=0}^{n-1} a_i \cdot b_i,$$

где сложение и умножение проводятся в поле $\mathbb{F}_2$.

Весом булевой функции f будем называть количество 1 в ее табличной записи и обозначать $wt(f)$.

Определение 1. Векторной булевой функцией (или (n, m)-функцией) S называется отображение $V_n \to V_m$, $n, m \in \mathbb{N}$.

Любую векторную булеву функцию S можно представить в виде упорядоченного набора ее *координатных функций*: $S(x) = (f_1(x), f_2(x), \ldots, f_m(x))$, где $x \in V_n$, $f_i(x)$ — булевы функции, $i \in \overline{1, m}$.

Если значения n и m понятны из контекста, вместо термина «(n, m)-функция» будем использовать термин «функция». Подстановка — элемент симметрической группы $S(V_n)$, или биективная (n, n)-функция.

Определение 2. Значение преобразования Уолша – Адамара (WHT) $W_S(a, b)$ (n, m)-функции S для значений $a \in V_n$, $b \in V_m$ определяется равенством

$$W_S^{a,b} = \sum_{x \in V_n} (-1)^{\langle a, x\rangle + \langle b, S(x)\rangle}.$$

Определение 3. Для (n, m)-функции S ее линейность L_S определяется равенством

$$L_S = \frac{1}{2} \max_{\substack{a \in V_n, \\ b \in V_m \setminus \theta}} \left| W_S^{a,b} \right|.$$

Нелинейность (n, m)-функции S обозначается N_S и определяется равенством

$$N_S = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in V_n, \\ b \in V_m \setminus \theta}} \left| W_S^{a,b} \right|.$$

Нелинейность (n, m)-функции характеризуется ее удаленностью от множества линейных функций той же размерности [19]. Существуют векторные булевы функции $S : V_n \to V_m$, $n, m \in \mathbb{N}$, $m \leqslant n/2$, которые максимально удалены от множества всех линейных функций и называются бент-функциями. Их нелинейность равна $2^{n-1} - 2^{n/2-1}$. В данной работе наряду с широко используемым понятием нелинейности часто будет использоваться термин «линейность» для наглядности изложения.

Элементу $v \in V_{2m}$ можно поставить в соответствие пару элементов (x_1, x_2), $x_1, x_2 \in V_m$, по следующему правилу: если $v = (v_0, \ldots, v_{m-1}, v_m, \ldots, v_{2m-1})$, то $v \cong (x_1, x_2)$, где $x_1 = (v_0, \ldots, v_{m-1}) \in V_m$, $x_2 = (v_m, \ldots, v_{2m-1}) \in V_m$. Таким образом, задавая подстановку на множестве пар векторов (x_1, x_2), определяем подстановку пространства V_{2m}.

Определение 4. Пусть F_1, $F_2 \colon V_m \times V_m \to V_m$ — произвольные $(2m, m)$-функции. Определим преобразование $F(x_1, x_2) = (y_1, y_2)$, которое будем называть *F-конструкцией* (см. рисунок), следующей системой:

$$\begin{cases} y_1 = F_1(x_1, x_2), \\ y_2 = F_2(x_2, y_1). \end{cases} \tag{1}$$

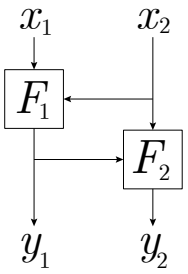

Рис. F-конструкция

Предложение 1. *Пусть F_1, $F_2 \colon V_m \times V_m \to V_m$ такие функции, для которых при произвольной фиксации z_2 функция $F_i(z_1, z_2)$, $i \in \overline{1,2}$, является биекцией по переменной z_1. Тогда*

1) *преобразование F является подстановкой на множестве $V_m \times V_m$,*

2) *общее количество подстановок F, которые определяются формулами (1), равно $(2^m!)^{2^{m+1}}$.*

Доказательство. Доказательство п. 1) можно найти, например, в [15].

Докажем п. 2). По условию предложения функции $F_i(z_1, z_2)$, $i = \overline{1,2}$, являются подстановками пространства V_m по переменной z_1 при фиксации переменной z_2. Для задания каждой из двух функций $F_i(z_1, z_2)$, $i \in \overline{1,2}$, необходимо фиксировать 2^m подстановок произвольным способом. Так как функции $F_1(z_1, z_2)$ и $F_2(z_1, z_2)$ выбираются независимо, то общее количество подстановок не превышает $(2^m!)^{2^{m+1}}$. Покажем, что разным парам функций F_1 и F_2 соответствуют различные подстановки множества $V_n \times V_n$.

Пусть даны две пары функций F'_j и F''_j, $j \in \{1, 2\}$. Если функции F'_1 и F''_2 не тождественно равны, то существует такое значение x_2, что $F'_1(x_1, x_2) \neq F''_1(x_1, x_2)$ для некоторого x_1, и тогда значения y_1, которые определяются формулой (1), будут разными, откуда следует, что две пары функций задают разные подстановки.

Пусть теперь $F'_1 = F''_1$ и $F'_2 \neq F''_2$. Тогда существует такое значение y_1, что $F'_2(y_1, x_2) \neq F''_2(y_1, x_2)$, и так как $F'_1 = F''_1$, то две пары функций задают разные y_2 в формуле (1). □

Преобразования такого вида широко известны в литературе: они возникают при декомпозиции подстановок (так называемая TU-декомпозиция). Самыми яркими примерами являются подстановка отечественного алгоритма шифрования «Кузнечик» [15] и дифференциально 2-равномерная подстановка пространства V_6 [17]. Тот факт, что данная конструкция позволяет получать подстановки с криптографическими характеристиками, которые либо являются оптимальными в некотором смысле, либо позволяют строить стойкие криптографические преобразования, стал причиной возросшего количества исследований этой конструкции.

Далее рассмотрим способ выбора функций F_1 и F_2, позволяющий гарантировать некоторые криптографические характеристики подстановок, построенных с использованием системы (1).

2. О способе задания функций переопределением значений

Построение сбалансированных (n, m)-функций, имеющих нелинейность не ниже некоторой границы $\mathbf{N}$, является сложной задачей при больших значениях границы $\mathbf{N}$ и при $n \geqslant 8$ и $m \geqslant 4$. Одним из известных подходов является построение сбалансированных (n, m)-функций

из несбалансированных (n, m)-функций, имеющих высокую нелинейность (см., например, [18]); он будет использоваться в данной работе при выборе функций F_i, $i \in \overline{1,2}$, в формуле (1).

Пусть $s'(x, y)$ — функция $V_m \times V_m \to V_m$, и для некоторого $\dot{y} \in V_m$ функция $s'(x, \dot{y})$ не является подстановкой по переменной x. Такое значение $\dot{y}$ будем называть выколотой точкой функции s'. Множество выколотых точек функции s' будем обозначать $\dot{Y} \subseteq V_m$:

$$\dot{Y} = \{\dot{y} \colon |\{s'(x, \dot{y}), x \in V_m\}| < 2^m\}.$$

Если множество $\dot{Y}$ не пусто, то можно переопределить функцию в каждой выколотой точке $\dot{y} \in \dot{Y}$ и получить такую новую функцию $s(x, y)$, что $s \colon V_m \times V_m \to V_m$ является подстановкой по переменной $x \in V_m$ при фиксации y любым значением из V_m. Пусть $\widehat{\pi}_y(x)$, $y \in \dot{Y}$, — совокупность подстановок пространства V_m, зададим $(2m, m)$-функцию s следующим образом:

$$s(x, y) = \begin{cases} s'(x, y), & y \notin \dot{Y}, \\ \widehat{\pi}_y(x), & y \in \dot{Y}. \end{cases} \tag{2}$$

Для оценки нелинейности функции $s(x, y)$ необходимо уметь вычислять коэффициенты Уолша – Адамара этой функции. Для функций $s'(x, \dot{y})$, $\dot{y} \in \dot{Y}$, как функций одной переменной x введем обозначение $g_{\dot{y}}(x)$.

Предложение 2. *Пусть $s'(x, y)$ — $(2m, m)$-функция с множеством выколотых точек $\dot{Y}$, а $\widehat{\pi}_{\dot{y}}$ — множество подстановок на V_m, $\dot{y} \in \dot{Y}$. Определим $(2m, m)$-функцию $s(x, y)$ без выколотых точек формулой (2). При $\alpha, \beta, \gamma \in V_m$ коэффициенты Уолша – Адамара функции s вычисляются по следующей формуле*:

$$W_s^{\alpha \| \beta, \gamma} = \begin{cases} W_{s'}^{\alpha \| \beta, \gamma} + \sum\limits_{\dot{y} \in \dot{Y}} (-1)^{\langle \beta, \dot{y} \rangle} \left(W_{\widehat{\pi}_{\dot{y}}}^{\alpha, \gamma} - W_{g_{\dot{y}}}^{\alpha, \gamma} \right), & \alpha \neq \theta, \\ W_{s'}^{\alpha \| \beta, \gamma} + \sum\limits_{\dot{y} \in \dot{Y}} (-1)^{\langle \beta, \dot{y} \rangle} \left(2 \cdot \mathrm{wt}\left(\langle \gamma, g_{\dot{y}}(x) \rangle \right) - 2^m \right), & \alpha = \theta, \gamma \neq \theta, \\ W_{s'}^{\alpha \| \beta, \gamma}, & \alpha = \theta, \gamma = \theta. \end{cases} \tag{3}$$

Доказательство. Вычислим коэффициенты Уолша – Адамара

согласно определению 2:

$$W_s^{\alpha\|\beta,\gamma} = \sum_{x,y\in V_m} (-1)^{\langle\alpha,x\rangle+\langle\beta,y\rangle+\langle\gamma,s(x,y)\rangle}$$

$$= \sum_{\substack{x,y\in V_m\\ y\notin\dot{Y}}} (-1)^{\langle\alpha,x\rangle+\langle\beta,y\rangle+\langle\gamma,s'(x,y)\rangle} + \sum_{\substack{x\in V_m\\ \dot{y}\in\dot{Y}}} (-1)^{\langle\alpha,x\rangle+\langle\beta,\dot{y}\rangle+\left\langle\gamma,\widehat{\pi}_{\dot{y}}(x)\right\rangle}$$

$$= \sum_{x,y\in V_m} (-1)^{\langle\alpha,x\rangle+\langle\beta,y\rangle+\langle\gamma,s'(x,y)\rangle} + \sum_{\dot{y}\in\dot{Y}}(-1)^{\langle\beta,\dot{y}\rangle} \sum_{x\in V_m} (-1)^{\langle\alpha,x\rangle+\left\langle\gamma,\widehat{\pi}_{\dot{y}}(x)\right\rangle}$$

$$-\sum_{\dot{y}\in\dot{Y}}(-1)^{\langle\beta,\dot{y}\rangle} \sum_{x\in V_m} (-1)^{\langle\alpha,x\rangle+\left\langle\gamma,g_{\dot{y}}(x)\right\rangle} = W_{s'}^{\alpha\|\beta,\gamma} + \sum_{\dot{y}\in\dot{Y}}(-1)^{\langle\beta,\dot{y}\rangle} \left(W_{\widehat{\pi}_{\dot{y}}}^{\alpha,\gamma} - W_{g_{\dot{y}}}^{\alpha,\gamma}\right),$$

что доказывает первое равенство в формуле (3).

Докажем второе равенство в формуле (3) — рассмотрим случай $\alpha = \theta$ и $\gamma \neq \theta$. Так как

$$W_f^{\theta,\gamma} = 2^m - 2\cdot \mathrm{wt}\left(\langle\gamma, f(x)\rangle\right),$$

где f — произвольная (m, m)-функция, то

$$W_s^{\theta\|\beta,\gamma} = W_{s'}^{\theta\|\beta,\gamma} + \sum_{\dot{y}\in\dot{Y}}(-1)^{\langle\beta,\dot{y}\rangle}\left(2\cdot \mathrm{wt}\left(\langle\gamma, g_{\dot{y}}(x)\rangle\right) - 2^m\right).$$

Докажем третье равенство в формуле (3). Если значения α и γ равны θ, то $W_{\widehat{\pi}_{\dot{y}}}^{\alpha,\gamma} = W_{g_{\dot{y}}}^{\alpha,\gamma}$ и $W_s^{\theta\|\beta,\theta} = W_{s'}^{\theta\|\beta,\theta}$, что и требовалось доказать. □

С помощью доказанного предложения можно получить следующую оценку линейности функции s, построенной по формуле (2).

Следствие 1. *В условиях предложения 2 верна следующая оценка сверху линейности L_s функции s:*

$$L_s \leqslant \max\left\{L_{s'} + \sum_{\dot{y}\in\dot{Y}}\left(L_{\widehat{\pi}_{\dot{y}}} + L_{g_{\dot{y}}(x)}\right), L_{s'} + \sum_{\dot{y}\in\dot{Y}}\left|2^m - 2\min_{\gamma\in V_m\setminus\theta}\mathrm{wt}\left(\langle\gamma, g_{\dot{y}}(x)\rangle\right)\right|\right\}.$$

Доказательство. Для доказательства следствия достаточно воспользоваться неравенством треугольника, определением 3 и формулой (3). □

Пусть требуется построить функцию s с линейностью не выше некоторой границы $\mathbf{L}$. Тогда можно искать такие функции s' и $\widehat{\pi}_y$, что верх-

няя граница, полученная в следствии 1, будет меньше $\mathbf{L}$. Так как каждое слагаемое в

$$\sum_{\dot{y}\in\dot{Y}}\left(L_{\widehat{\pi}_{\dot{y}}}+L_{g_{\dot{y}}(x)}\right) \text{ и } \sum_{\dot{y}\in\dot{Y}}\left|2^m-2\cdot\mathrm{wt}\left(g_{\dot{y}}\left(x\right)\right)\right|$$

является неотрицательным целым числом (или даже положительным, так как для любой подстановки π ее линейность больше 0, $L_\pi>0$), то при одном и том же значении линейности функции s' функция s, полученная по формуле (2), потенциально имеет тем большую линейность, чем больше выколотых точек у функции s'.

Действительно, пусть дана $(2m,m)$-функция s', имеющая ровно одну выколотую точку $\dot{y}$. Обозначим $g(x)=s\left(x,\dot{y}\right)$, и пусть $\widehat{\pi}$ — подстановка на V_m. Определим $(2m,m)$-функцию s, не имеющую выколотых точек, следующим образом:

$$s(x,y)=\begin{cases}s'(x,y), & y\neq\dot{y},\\ \widehat{\pi}(x), & y=\dot{y}.\end{cases} \tag{4}$$

Для таких функций можно получить потенциально меньшую оценку линейности L_s.

Следствие 2. *Пусть s — $(2m,m)$-функция, заданная формулой (4). Тогда верна следующая верхняя оценка линейности L_s функции s:*

$$L_s\leqslant\max\left\{L_{s'}+L_{\widehat{\pi}}+L_g,L_{s'}+\left|2^m-2\cdot\min_{\gamma\in V_m\setminus\theta}\mathrm{wt}\left(\langle\gamma,g(x)\rangle\right)\right|\right\}.$$

В связи со следствием 2 наибольший интерес представляют функции s', которые имеют только одну выколотую точку $\dot{y}$.

Покажем, что при дополнительных ограничениях на функцию g (например, если функция $g(x)$ является константой) удается уточнить верхнюю оценку линейности функции s.

Предложение 3. *Пусть s' — $(2m,m)$-функция, имеющая ровно одну выколотую точку $\dot{y}$, $g(x)=s'\left(x,\dot{y}\right)$, $\widehat{\pi}$ — подстановка на V_m, и $(2m,m)$-функция s определяется формулой (4).*

Тогда если функция $g(x)$ есть константа, то коэффициенты Уолша – Адамара функции $s(x,y)$ для произвольных $\alpha,\beta,\gamma\in V_m$ вычисляются по следующей формуле:

$$W_s^{\alpha\|\beta,\gamma}=\begin{cases}W_{s'}^{\alpha\|\beta,\gamma}+(-1)^{\langle\beta,\dot{y}\rangle}\cdot W_{\widehat{\pi}}^{\alpha,\gamma}, & \alpha\neq\theta,\\ 0, & \alpha=\theta,\gamma\neq\theta,\\ W_{s'}^{\theta\|\beta,\theta}, & \alpha=\theta,\gamma=\theta.\end{cases} \tag{5}$$

Доказательство. Доказательство проведем аналогично доказательству предложения 2:

$$W_s^{\alpha\|\beta,\gamma} = W_{s'}^{\alpha\|\beta,\gamma} + (-1)^{\langle\beta,\dot{y}\rangle}\left(W_{\widehat{\pi}}^{\alpha,\gamma} - \sum_{x\in V_m}(-1)^{\langle\alpha,x\rangle+\langle\gamma,g(x)\rangle}\right). \qquad (6)$$

Докажем первое равенство в выражении (5). Если $\alpha \neq \theta$, то

$$\sum_{x\in V_m}(-1)^{\langle\alpha,x\rangle+\langle\gamma,g(x)\rangle} = (-1)^c \sum_{x\in V_m}(-1)^{\langle\alpha,x\rangle} = \theta,$$

где $c \in \{0,1\}$; отсюда и из (6) получаем первое равенство.

Рассмотрим случай $\alpha = \theta$, $\gamma \neq \theta$. Теперь $W_{\widehat{\pi}}^{\alpha,\gamma} = 0$ и

$$\sum_{x\in V_m}(-1)^{\langle\alpha,x\rangle+\langle\gamma,g(x)\rangle} = (-1)^c \cdot 2^m,$$

где $c \in \{0,1\}$. Покажем, что если $\gamma \neq \theta$, то $W_{s'(x,y)}^{\theta\|\beta,\gamma} = (-1)^c \cdot 2^m \cdot (-1)^{\langle\beta,\dot{y}\rangle}$, что докажет второе равенство в выражении (5):

$$\begin{aligned} W_{s'}^{\theta\|\beta,\gamma} &= \sum_{x,y\in V_m}(-1)^{\langle\beta,y\rangle+\langle s'(x,y),\gamma\rangle} = \sum_{y\in V_m}(-1)^{\langle\beta,y\rangle}\sum_{x\in V_m}(-1)^{\langle s'(x,y),\gamma\rangle} \\ &= \sum_{y\neq\dot{y}}(-1)^{\langle\beta,y\rangle}\sum_{x\in V_m}(-1)^{\langle s'(x,y),\gamma\rangle} + (-1)^{\langle\beta,\dot{y}\rangle}\sum_{x\in V_m}(-1)^{\langle g(x),\gamma\rangle} \\ &= 0 + (-1)^c \cdot 2^m \cdot (-1)^{\langle\beta,\dot{y}\rangle}. \end{aligned}$$

Третье равенство в формуле (5) является прямым следствием предложения 2. □

Покажем, что существуют такие функции s', что функция $g(x)$ является константой, а сама функция s' имеет достаточно высокую нелинейность. Например, произвольная $(2m, m)$ бент-функция с одной выколотой точкой (см. [20]) обладает таким свойством.

Предложение 4. *Пусть $b(x,y)\colon V_m \times V_m \to V_m$ — бент-функция, имеющая ровно одну выколотую точку $\dot{y}$. Тогда функция $g(x) = b(x,\dot{y})$ является константой.*

Доказательство. Рассмотрим произвольную невырожденную линейную комбинацию координатных функций $b(x,y)$:

$$f(x,y) = \langle\alpha, b(x,y)\rangle, \alpha \neq \theta.$$

Так как $f(x, y)$ — бент-функция, то известно (см., например, [20]), что ее вес равен либо $2^{2m-1}+2^{m-1}$, либо $2^{2m-1}-2^{m-1}$. Если функция $b(x, y)$ имеет ровно одну выколотую точку, то при фиксации $y \neq \dot{y}$ функция $b(x, y)$ есть биекция по переменной x. Тогда вес функции $f(x, y)$, как функции от переменной x при $y \neq \dot{y}$, равен 2^{m-1}. Суммарный вес всех таких функций равен

$$(2^m - 1) \cdot 2^{m-1} = 2^{2m-1} - 2^{m-1}.$$

Отсюда получаем, что вес функции $f(x, \dot{y})$ равен либо 0, либо 2^m, что доказывает предложение. □

Следствие 3. *В условиях предложения 3 верхняя и нижняя границы линейности L_s функции s задаются следующими неравенствами:*

$$L_{s'} - L_{\widehat{\pi}} \leqslant L_s \leqslant L_{s'} + L_{\widehat{\pi}}.$$

Если s' — векторная бент-функция, то

$$L_{s'} < L_s \leqslant L_{s'} + L_{\widehat{\pi}}.$$

Доказательство. Для доказательства первого неравенства необходимо воспользоваться неравенствами

$$|a + b| \leqslant |a| + |b|, \ \ |a + b| \geqslant |a| - |b|,$$

определением 3 и первыми двумя равенствами в формуле (5).

Второе неравенство следует из первого и того факта, что линейность сбалансированной функции s больше линейности бент-функции s'. □

В частности, следствие 3 гарантирует способ построения $(2m, m)$-функции s по формуле (4) с нелинейностью не ниже $L_s \leqslant L_{s'} + L_{\widehat{\pi}}$. В случае $m = 4$ наименьшее возможное значение $L_{\widehat{\pi}}$ равно 4. Тогда, используя в качестве s' бент-функции, можно получить $(8, 4)$-функцию, имеющую линейность 12.

Обратное тоже верно. Пусть выбрана некоторая граница $\mathbf{L}$ и требуется построить $(2m, m)$-функции, имеющие линейность не выше $\mathbf{L}$. Тогда, выбирая подстановки, имеющие наименьшее возможное значение $L_{\widehat{\pi}}$, и выбрав $(2m, m)$-функцию s', имеющую ровно одну выколотую точку $\dot{y}$ и для этой точки $s'(x, \dot{y}) = \text{const}$, а линейность s' не выше $\mathbf{L} - L_{\widehat{\pi}}$, по следствию 3 можем построить $(2m, m)$-функцию s с линейностью не выше $\mathbf{L}$.

Приведем пример $(2m, m)$-функций s', имеющих ровно одну выколотую точку $\dot{y}$, и $s'(x, \dot{y}) = \text{const}$. Для рассмотренных функций в некоторых условиях доказано, что они имеют высокую нелинейность. Все эти функции можно использовать в качестве функций F_i в F-конструкции.

Пусть $n = 2m$, $x, y \in V_m$, $m \in \mathbb{N}$. Рассмотрим следующие функции (в их определениях мультипликативные операции проводятся над векторами как элементами поля $\mathbb{F}_{2^m}$):

– $s'(x, y) = L(x \cdot \pi(y)) + G(y)$, где $\pi, L \in S(V_m)$, G — произвольная (m, m)-функция. В случае когда L — линейная подстановка, s' является бент-функцией Майорана – Макфарленда [19],

– $s'(x, y) = P(x, y) + G(y)$, где G — произвольная (m, m)-функция, P — такая $(2m, m)$-функция, что $P(x, y)$ для любого фиксированного $x \neq \theta$ является подстановкой по y. В случае когда при фиксации $y \in V_m$ функция P линейна по переменной x, s' является бент-функцией, которую называют расширенной конструкцией Майорана – Макфарленда [19],

– $s'(x, y) = G(x \cdot y^{-1})$, где G — сбалансированная $(2m, m)$-функция. Тогда s' — бент-функция, которую называют PS_{ap} бент-функцией [19],

– $s'(x, y) = \pi_1(x) \cdot \pi_2(x)$, где $\pi_1, \pi_2 \in S(V_m)$. Если хотя бы одна из подстановок π_1 или π_2 является линейной, то функция s' является частным случаем конструкции Майорана – Макфарленда.

Этот список не исчерпывает все возможные конструкции. Многие известные классы $(2m, m)$-бент функций имеют ровно одну выколотую точку [20]. В то же время в этом списке приведены функции, которые при некоторых фиксациях параметров не являются бент-функциями и которые были использованы, например, в [5].

3. Использование функций с одной выколотой точкой в F-конструкции

Пусть s'_1 и s'_2 — две $(2m, m)$-функции, имеющие выколотые точки $\dot{y}_1$ и $\dot{y}_2$ соответственно, $\widehat{\pi}_1$ и $\widehat{\pi}_2$ — две подстановки пространства V_m. Зададим функции F_1 и F_2 согласно формуле (4) и определим подстановку $F \in S(V_{2m})$, $F(x_1, x_2) = (y_1, y_2)$, с помощью F-конструкции по

формуле (1):

$$y_1 = F_1(x_1, x_2) = \begin{cases} s'_1(x_1, x_2), & x_2 \neq \dot{y}_1, \\ \widehat{\pi}_1(x_1), & x_2 = \dot{y}_1, \end{cases} \tag{7}$$

$$y_2 = F_2(x_2, y_1) = \begin{cases} s'_2(x_2, y_1), & y_1 \neq \dot{y}_2, \\ \widehat{\pi}_2(x_2), & y_1 = \dot{y}_2. \end{cases} \tag{8}$$

Согласно используемым предположениям при фиксации произвольного $x_2 \neq \dot{y}_i$ функция $s'_i(x_1, x_2)$ (для произвольного $i \in \overline{1,2}$) является биекцией по переменной x_1. Тогда для $x_2 \neq \dot{y}_i$ корректно определены биективные отображения $s'^{-1}_i(y, x_2)$ как функции от одной переменной y при фиксированном $x_2 \neq \dot{y}_i$. Аналогично корректно определены функции $F_i^{-1}(y, x_2)$ как подстановки по переменной y при фиксированном значении $x_2 \in V_m$.

Выпишем выражение для подстановки $F^{-1}(y_1, y_2) = (x_1, x_2)$, обратной к заданной формулами (7)–(8) подстановке F:

$$x_2 = F_2^{-1}(y_1, y_2) = \begin{cases} s'^{-1}_2(y_2, y_1), & y_1 \neq \dot{y}_2, \\ \widehat{\pi}_2^{-1}(y_2), & y_1 = \dot{y}_2, \end{cases} \tag{9}$$

$$x_1 = F_1^{-1}(y_1, x_2) = \begin{cases} s'^{-1}_1(y_1, x_2), & x_2 \neq \dot{y}_1, \\ \widehat{\pi}_1^{-1}(y_1), & x_2 = \dot{y}_1. \end{cases} \tag{10}$$

При этом как F_2^{-1}, так и F_1^{-1} являются функциями с одной выколотой точкой вида (4), а значения y_2 и x_1 не выражаются напрямую через x_1, x_2 и y_1, y_2 соответственно. Например, y_2 выражается через x_1 и x_2 из (8) довольно громоздкой формулой:

$$y_2 = \begin{cases} s'_2(x_2, s'_1(x_1, x_2)), & x_2 \neq \dot{y}_1, s'_1(x_1, x_2) \neq \dot{y}_2, \\ s'_2(x_2, \widehat{\pi}_1(x_1)), & x_2 = \dot{y}_1, \widehat{\pi}_1(x_1) \neq \dot{y}_2, \\ \widehat{\pi}_2(x_2), & x_2 \neq \dot{y}_1, s'_1(x_1, x_2) = \dot{y}_2, \\ \widehat{\pi}_2(x_2), & x_2 = \dot{y}_1, \widehat{\pi}_1(x_1) = \dot{y}_2. \end{cases} \tag{11}$$

Задав ограничения на функции s'_1 и s'_2, можно упростить выражения для y_2 как функции от x_1, x_2 и для x_1 как функции от y_1, y_2 и привести его к виду (4).

Предложение 5. *Пусть подстановка $F(x_1, x_2) = (y_1, y_2)$ задается формулами (7)–(8). Пусть также*

1) $\widehat{\pi}_1(x_1) = \dot{y}_2 \Leftrightarrow F_1(x_1, x_2) = \dot{y}_2$,

2) $x_2 = \dot{y}_1 \Leftrightarrow F_2(x_2, y_1) = \widehat{\pi}_2(\dot{y}_1)$.

Тогда

а) y_2 *выражается через* x_1, x_2 *формулой*

$$y_2 = FI_2(x_1, x_2) = \begin{cases} s_2'(x_2, s_1'(x_1, x_2)), & x_1 \neq \widehat{\pi}_1^{-1}(\dot{y}_2), \\ \widehat{\pi}_2(x_2), & x_1 = \widehat{\pi}_1^{-1}(\dot{y}_2), \end{cases} \tag{12}$$

б) x_1 *выражается через* y_1, y_2 *формулой*

$$x_1 = FI_1(y_1, y_2) = \begin{cases} s_1'^{-1}\left(y_1, s_2'^{-1}(y_2, y_1)\right), & y_2 \neq \dot{y}_1, \\ \widehat{\pi}_1^{-1}(y_1), & y_2 = \dot{y}_1. \end{cases} \tag{13}$$

При выполнении условий предложения 5 подстановка $F(x_1, x_2) = (y_1, y_2)$ задается с помощью функций F_1 (см. формулу (7)) и FI_2 (см. формулу (12)), а обратная подстановка $F^{-1}(y_1, y_2) = (x_1, x_2)$ — с помощью функций F_2^{-1} (см. формулу (9)) и FI_1 (см. формулу (13)).

Замечание. Перед началом доказательства заметим, что функция $s_2'^{-1}(y_2, y_1)$, вообще говоря, не определена в точке $y_1 = \dot{y}_2$. Однако так как по формуле (7) $y_1 = F_1(x_1, x_2)$ и в силу первого условия предложения 5

$$y_1 = \dot{y}_2 \Leftrightarrow \widehat{\pi}_1(x_1) = \dot{y}_2,$$

то в точке $y_1 = \dot{y}_2$ функция $s_1'^{-1}\left(\dot{y}_2, s_2'^{-1}(y_2, \dot{y}_2)\right)$ является константой и равняется $\widehat{\pi}_1^{-1}(\dot{y}_2)$. Значение $s_2'^{-1}(y_2, y_1)$ в точке $y_1 = \dot{y}_2$ можно задать произвольно.

Аналогично функция $s_1'^{-1}\left(y_1, s_2'^{-1}(y_2, y_1)\right)$ не определена, если $s_2'^{-1}(y_2, y_1) = \dot{y}_1$, или $y_2 = s_2'(\dot{y}_1, y_1)$. Тогда при $y_1 \neq \dot{y}_2$ согласно условию 2) предложения 5 функция $s_1'^{-1}\left(y_1, s_2'^{-1}(y_2, y_1)\right)$ не зависит от $s_2'^{-1}(y_2, y_1)$, значение которой в точке $y_2 = \dot{y}_1$ можно задать произвольным способом.

Доказательство. Докажем формулу (12) непосредственной проверкой. Рассмотрим формулу (11). Так как $x_2 = \dot{y}_1 \Leftrightarrow F_2(x_2, y_1) = \widehat{\pi}_2(\dot{y}_1)$, то при $x_2 = \dot{y}_1$ значение $s_2'(x_2, \widehat{\pi}_1(x_1))$ не зависит от значения $\widehat{\pi}_1(x_1)$. Отсюда следует, что вместо

$$s_2'(x_2, \widehat{\pi}_1(x_1)), \ x_2 = \dot{y}_1, \ \widehat{\pi}_1(x_1) \neq \dot{y}_2$$

можно написать

$$s'_2\left(x_2, s'_1(x_1, x_2)\right),\ x_2 = \dot{y}_1,\ \widehat{\pi}_1(x_1) \neq \dot{y}_2.$$

Так как $\widehat{\pi}_1(x_1) = \dot{y}_2 \Leftrightarrow F_1\left(x_1, x_2\right) = \dot{y}_2$, то при $x_2 \neq \dot{y}_1$ и $s'_1(x_1, x_2) = \dot{y}_2$ верно равенство $\widehat{\pi}_1(x_1) = \dot{y}_2$, что доказывает справедливость формулы (12). Отсюда следует, что вместо

$$\widehat{\pi}_2\left(x_2\right),\ x_2 \neq \dot{y}_1,\ s'_1(x_1, x_2) = \dot{y}_2$$

можно написать

$$\widehat{\pi}_2\left(x_2\right),\ x_2 \neq \dot{y}_1,\ \widehat{\pi}_1(x_1) = \dot{y}_2.$$

Последнее доказывает справедливость формулы (12).

Для доказательства п. б) переформулируем условия 1) и 2) доказываемого предложения для функции F^{-1}:

1) $y_1 = \dot{y}_2 \Leftrightarrow F^{-1}\left(y_1, x_2\right) = \widehat{\pi}^{-1}\left(\dot{y}_2\right)$,

2) $\widehat{\pi}_2^{-1}\left(y_2\right) = \dot{y}_1 \Leftrightarrow F_2^{-1}\left(y_2, y_1\right) = \dot{y}_1$.

Теперь формула (13) доказывается аналогично с учетом замечания.

□

При выполнении условий предложения 5 подстановка $F(x_1, x_2) = (y_1, y_2)$ задается формулами (7) и (12), а обратная подстановка $F^{-1}(y_1, y_2) = (x_1, x_2)$ задается формулами (9) и (13). Каждая из этих формул задается формулой вида (4) при помощи функций с одной выколотой точкой. Перечислим эти функции:

– y_1 при $x_2 \neq \dot{y}_1$ задается формулой $s'_1\left(x_1, x_2\right)$,

– y_2 при $x_1 \neq \widehat{\pi}^{-1}\left(\dot{y}_1\right)$ задается формулой $s'_2\left(x_2, s'_1(x_1, x_2)\right)$,

– x_1 при $y_2 \neq \dot{y}_1$ задается формулой $s_1'^{-1}\left(y_1, s_2'^{-1}(y_2, y_1)\right)$,

– x_2 при $y_1 \neq \dot{y}_2$ задается формулой $s_2'^{-1}\left(y_2, y_1\right)$.

4. Алгоритм построения подстановки с линейностью не выше заданной

Так как нелинейность F равняется нелинейности F^{-1}, то можно предложить следующий алгоритм построения подстановки с линейностью не выше $\mathbf{L}$ на основе предложений 3 и 5. Сначала необходимо фиксировать параметры алгоритма $\mathbf{L}_1 \leqslant \mathbf{L}_2 < \mathbf{L}$, $\mathbf{L} - \mathbf{L}_2 = \mathbf{L}_\pi$. При

этом должны существовать такие подстановки пространства V_m, что их линейность не превосходит значения $\mathbf{L}_\pi$.

Алгоритм 1

1) Выбрать такую функцию $s'_1(x_1, x_2)$ с единственной выколотой точкой $x_2 = \dot{y}_1$, что:
   a) $s'_1(x_1, \dot{y}_1) = \text{const}$,
   b) существует такое z_1, что при $x_2 \neq \dot{y}_1$ функция $s'_1(z_1, x_2)$ есть некоторая константа $\dot{y}_2$,
   c) $L_{s'} \leqslant \mathbf{L}_1$.
2) Выбрать такую функцию $s'^{-1}_2(y_2, y_1)$ с единственной выколотой точкой $y_2 = \dot{y}_2$, что:
   a) $s'^{-1}_2(y_2, \dot{y}_2) = \text{const}$,
   b) существует такое z_2, что при $y_1 \neq \dot{y}_2$ верно равенство $s'^{-1}_2(z_2, y_1) = \dot{y}_1$,
   c) $L_{s'^{-1}_2} \leqslant \mathbf{L}_1$.
3) Построить функцию $s''_2(x_2, x_1) = s'_2(x_2, s'_1(x_1, x_2))$ и проверить выполнение неравенства $L_{s''_2} \leqslant \mathbf{L}_2$. Если выполняется, то перейти на следующий шаг, иначе перейти на шаг 2.
4) Построить функцию $s''_1(y_1, y_2) = s'^{-1}_1\left(y_1, s'^{-1}_2(y_2, y_1)\right)$ и проверить выполнение неравенства $L_{s''_1} \leqslant \mathbf{L}_2$. Если выполняется, то подать функции s'_1, s'^{-1}_2 на выход, иначе перейти на шаг 2.
5) Выбрать такую подстановку $\widehat{\pi}_1(x)$, что
   a) $z_1 = \widehat{\pi}^{-1}_1(\dot{y}_2)$,
   b) $L_{\widehat{\pi}_1} \leqslant \mathbf{L}_\pi$,

   и построить функцию $F_1(x_1, x_2)$, используя формулу (7).
6) Выбрать такую подстановку $\widehat{\pi}_2(x)$, что
   a) $z_2 = \widehat{\pi}_2(\dot{y}_1)$,
   b) $L_{\widehat{\pi}_2} \leqslant \mathbf{L}_\pi$,

и построить функцию $F_2(x_1, x_2)$, используя формулу (8).

7) Построить подстановку F, используя формулу (1), и проверить выполнение условия $L_F \leqslant \mathbf{L}$. Если оно выполняется, то подать функцию F на выход, иначе перейти на шаг 5.

Тогда по предложению 3 для любой такой подстановки $\widehat{\pi}_1(x)$, что $z_1 = \widehat{\pi}_1^{-1}(\dot{y}_2)$, и подстановки $\widehat{\pi}_2(x)$, что $z_2 = \widehat{\pi}_2(\dot{y}_1)$, линейность каждой из функций s'_1, $s_2'^{-1}$, s''_1 и s''_2 будет не больше $\mathbf{L}_2 + \max\{L_{\widehat{\pi}_1}, L_{\widehat{\pi}_2}\}$.

Покажем, что выбор функций s'_1 и $s_2'^{-1}$ можно проводить независимо. Заметим, что для функций s'_1 и $s_2'^{-1}$ шаги 1.a и 1.c алгоритма эквивалентны шагам 2.a и 2.c. Разница только в шагах 1.b и 2.b в фиксации конкретных значений аргументов.

Пусть имеется такая функция $s'_1(x_1, x_2)$ с единственной выколотой точкой $x_2 = \dot{y}_1$, удовлетворяющая условиям 2.a, 2.b, 2.c алгоритма 1. Тогда функция

$$s_2'^{-1}(y_2, y_1) = s'_1(y_2 + z_1 + z_2, y_1 + \dot{y}_1 + \dot{y}_2) + \dot{y}_2 + \dot{y}_1$$

имеет единственную выколотую точку $y_2 = \dot{y}_2$ и удовлетворяет условиям 2.a, 2.b, 2.c алгоритма.

Этот факт позволяет проводить поиск функций, удовлетворяющих условиям 1.a, 1.b, 1.c алгоритма, на предварительном этапе для выработки большого количества подстановок.

Для нахождения линейности подстановки F необходимо вычислить $2^{2m}(2^{2m} - 1)$ значений $W_F^{a,b}$, $a \in V_{2m}$, $b \in V_{2m}\backslash\theta$. Шаги 1–6 алгоритма позволяют строить функции s'_1, $s_2'^{-1}$, s''_1 и s''_2 с линейностью не ниже $\mathbf{L}$. Тогда:

– из $L_{s'_1} \leqslant \mathbf{L}$ следует, что $1/2 \cdot W_F^{\alpha\|\beta,\gamma\|\theta} \leqslant \mathbf{L}$, $\alpha, \beta \in V_m$, $\gamma \in V_m\backslash\theta$,

– из $L_{s''_2} \leqslant \mathbf{L}$ следует, что $1/2 \cdot W_F^{\alpha\|\beta,\theta\|\delta} \leqslant \mathbf{L}$, $\alpha, \beta \in V_m$, $\delta \in V_m\backslash\theta$,

– из $L_{s_2'^{-1}} \leqslant \mathbf{L}$ следует, что $1/2 \cdot W_F^{\theta\|\beta,\gamma\|\delta} \leqslant \mathbf{L}$, $\beta \in V_m\backslash\theta$, $\gamma\|\delta \in V_{2m}$,

– из $L_{s''_1} \leqslant \mathbf{L}$ следует, что $1/2 \cdot W_F^{\alpha\|\theta,\gamma\|\delta} \leqslant \mathbf{L}$, $\alpha \in V_m\backslash\theta$, $\gamma\|\delta \in V_{2m}$.

Поэтому не менее

$$2 \cdot (2^m - 1) \cdot 2^{2m} + 2 \cdot (2^m - 1)\left(2^{2m} - 1\right) - 4 \cdot (2^m - 1)^2 = O\left(2^{3m+2}\right)$$

значений $W_F^{a,b}$ будут меньше $\mathbf{L}$.

Пример. Как было сказано выше, функции вида $f(x, y) = \pi(x) \cdot y$ являются бент-функциями с единственной выколотой точкой $\dot{y} = \theta$. При этом если $\pi(x) = \theta$, то $f(x, y) = \theta$. Зададим функции $F_1(x_1, x_2)$, $F_2^{-1}(y_1, y_2)$:

$$F_1(x_1, x_2) = \begin{cases} \pi_1(x_1) \cdot x_2, & x_2 \neq \theta, \\ \widehat{\pi}_1(x_1), & x_2 = \theta, \end{cases}$$

$$F_2^{-1}(y_1, y_2) = \begin{cases} \pi_2(y_1) \cdot y_2, & y_2 \neq \theta, \\ \widehat{\pi}_2(y_1), & y_2 = \theta. \end{cases}$$

Выразим y_1 через x_1, x_2. Рассмотрим случай $x_2 \neq \theta$, $y_2 \neq \theta$. Тогда

$$x_2 = \pi_2(y_1) \cdot y_2 = \pi_2(y_1) \cdot \pi_1(x_1) \cdot x_2 \Rightarrow y_1 = \pi_2^{-1}\left(\frac{1}{\pi_1(x_1)}\right).$$

Получили, что значение y_1 не зависит от x_2 и вычисляется с использованием некоторой подстановки по переменной x_1; это позволяет утверждать, что данная конструкция заведомо неприменима для синтеза стойких криптографических алгоритмов.

Приведенный пример показывает, что при построении подстановки с использованием конструкции, определяемой формулой (1), необходимо внимательно подходить к выбору функций F_1 и F_2 и даже лучший (с некоторой точки зрения) выбор функций s_1' и $s_2'^{-1}$ может привести к невозможности построения подстановки с приемлемыми криптографическими характеристиками. В то же время, в [5] было показано, что при подходящем выборе функций F_1 и F_2 можно построить подстановки с высокой нелинейностью.

Заключение

В работе предложен алгоритм построения подстановки с линейностью не выше заданной. Доказан ряд утверждений, обосновывающих корректность предложенного алгоритма.

Список литературы

[1] Yu Y., Wang M., Li Y., *Constructing differential 4-uniform permutations from know ones*, IACR Cryptology ePrint Archive, 2011:047, 2011 http://eprint.iacr.org/2011/047.

[2] Fu S., Feng X., Wu B., *Differentially 4-uniform permutations with the best known nonlinearity from Butterflies*, IACR Cryptology ePrint Archive, 2017:449, 2017 http://eprint.iacr.org/2017/449.

[3] de la Cruz Jiménez R.A., *On some methods for constructing almost optimal S-Boxes and their resilience against side-channel attacks*, IACR Cryptology ePrint Archive, 2018:618, 2018 https://eprint.iacr.org/2018/618.

[4] Peng J., Tan C., "New differentially 4-uniform permutations by modifying the inverse function on subfields.", *Cryptography and Communications*, **9**:3 (2017), 363–378.

[5] Fomin D. B., "New classes of 8-bit permutations based on a butterfly structure", *Математические вопросы криптографии*, **10**:2 (2019), 169–180.

[6] Canteaut A., Duval S., Leurent G., *Construction of lightweight s-boxes using Feistel and MISTY structures* (*full version*), IACR Cryptology ePrint Archive, 2015:711, 2015 http://eprint.iacr.org/2015/711.

[7] Lim C.-H., *CRYPTON*: *A new* 128*-bit block cipher — specification and analysis*, 1998 http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.52.5771&rep=rep1&type=pdf.

[8] Gérard B., Grosso V., Naya-Plasencia M., Standaert F.-X., "Block ciphers that are easier to mask: How far can we go?", Lect. Notes Comput. Sci., **8086**, 2013, 383–399.

[9] Matsui M., "New block encryption algorithm MISTY", Lect. Notes Comput. Sci., **1267**, 1997, 54–68.

[10] Grosso V., Leurent G., Standaert F.-X., Varici K."Ls-designs: Bitslice encryption for efficient masked software implementations.", Lect. Notes Comput. Sci., **8540**, 2014, 18–37.

[11] Standaert F.-X., Piret G., Rouvroy G., Quisquater J.-J., Legat J.-D., "ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware", Lect. Notes Comput. Sci., **3017**, 2004, 279–299.

[12] Rijmen V., Barreto P., *The KHAZAD block cipher*, NESSIE Proposal, 2000.

[13] Lim C.H., "A revised version of Crypton — Crypton v1.0", Lect. Notes Comput. Sci., **1636**, 1999, 31–45.

[14] Stallings W., "The Whirlpool secure hash function", *Cryptologia*, **30**:1 (2006), 55–67.

[15] Biryukov A., Perrin L., Udovenko A., "Reverse-engineering the S-box of Streebog, Kuznyechik and STRIBOBr1", Lect. Notes Comput. Sci., **9665**, 2016, 372–402.

[16] Perrin L., *Cryptanalysis*, *Reverse-Engineering and Design of Symmetric Cryptographic Algorithms*, Univ. Luxembourg, 2017 http://hdl.handle.net/10993/31195.

[17] Perrin L., Udovenko A., Biryukov A., "Cryptanalysis of a Theorem: decomposing the only known solution to the Big APN Problem", Lect. Notes Comput. Sci., **9815**, 2016, 93–122.

[18] Dobbertin H., "Construction of bent functions and balanced boolean functions with high nonlinearity", Lect. Notes Comput. Sci., **1008**, 1994, 61–74.

[19] Carlet C., Crama Y., Hammer P.L., "Vectorial Boolean functions for cryptography", *Boolean Models and Methods in Mathematics*, Cambridge Univ. Press, 2010, 398–470.

[20] Mesnager S., *Bent Functions. Fundamentals and Results*, Springer, 2016, 544 pp.