В работе рассмотрены новые методы синтеза нелинейных элементов современных шифров — криптографических S-блоков подстановки. Представлены методы синтеза, основанные на строгом описании криптографических свойств S-блоков подстановки, с использованием математического аппарат теории булевых функций. Показаны примеры синтеза S-блоков подстановки, которые удовлетворяют таким базовым критериям криптографического качества как: высокая нелинейность, отсутствие корреляции между выходом и входом S-блока подстановки, строгий лавинный критерий и др. Показано, что криптографическое качество S-блоков подстановки существенно улучшаются с ростом их длины. Приведены методы, которые позволяют синтез S-блоков подстановки любой длины, которая может быть реализована вычислительной техникой.

Соколов Артём Викторович, 24 года, PhD (кандидат технических наук), Одесский национальный политехнический университет, г.Одесса, Украина. Основная область научных интересов: проблемы защиты информации с использованием совершенных алгебраических конструкций. Инструктор детской Йоги, увлекается игрой на фортепиано, классической музыкой.

978-3-659-67440-2

Нелинейные преобразования

Соколов

Артём Соколов

Новые методы синтеза нелинейных преобразований современных шифров

LAP LAMBERT Academic Publishing

Артём Соколов

Новые методы синтеза нелинейных преобразований современных шифров

Артём Соколов

Новые методы синтеза нелинейных преобразований современных шифров

LAP LAMBERT Academic Publishing

Impressum / Выходные данные
Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Библиографическая информация, изданная Немецкой Национальной Библиотекой. Немецкая Национальная Библиотека включает данную публикацию в Немецкий Книжный Каталог; с подробными библиографическими данными можно ознакомиться в Интернете по адресу http://dnb.d-nb.de.

Coverbild / Изображение на обложке предоставлено: www.ingimage.com

Verlag / Издатель:
LAP LAMBERT Academic Publishing
ist ein Imprint der / является торговой маркой
OmniScriptum GmbH & Co. KG
Heinrich-Böcking-Str. 6-8, 66121 Saarbrücken, Deutschland / Германия
Email / электронная почта: info@lap-publishing.com

Herstellung: siehe letzte Seite /
Напечатано: см. последнюю страницу
ISBN: 978-3-659-67440-2

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

В условиях тотальной информатизации и компьютеризации общества, сопровождающейся постоянным ростом объема конфиденциальных данных, все более остро встает проблема широкого применения криптографической защиты информации. Все более повсеместно для организации связи и хранения данных, требующих защиты, используются блочные и поточные криптографические алгоритмы, которые должны обладать высоким уровнем надежности и хорошим быстродействием. Такое положение дел диктует необходимость более тщательного изучения возможностей улучшения криптографического качества и ресурсоемкости базовых компонентов (примитивов) существующих и разрабатываемых криптографических алгоритмов.

Одним из важнейших элементов многих блочных шифров, определяющим скоростные показатели и показатели надежности криптопреобразования в целом, является криптографический S-блок подстановки. Быстродействие и эффективность современных криптографических алгоритмов во многом определяется свойствами используемых в них нелинейных преобразований, то есть S-блоков подстановки. Это делает задачу повышения эффективности современных шифров на основе синтеза высококачественных S-блоков подстановки наиболее актуальной. Качество S-блоков подстановки определяется требованиями критериев криптографической стойкости конструкции, основанных на определенных видах атак криптоанализа (линейного, корреляционного, дифференциального) и показателями экономии аппаратных ресурсов, простоты реализации, скорости работы и возможности реализации параллельных схем вычислений.

Известно, что также как и в случае с помехоустойчивыми кодами, криптографическое качество S-блоков подстановки и их способность противостоять атакам криптоанализа значительно улучшается с ростом длины N.

Таким образом, актуальной является задача синтеза S-блоков подстановки большой длины, то есть, многобайтных.

С ростом длины S-блока подстановки очень сильно усложняются методы их синтеза. Данное обстоятельство органично ставит задачу синтеза больших S-блоков подстановки, а также разработки рекуррентных методов синтеза S-блоков подстановки.

Важную проблему представляют методы синтеза экономичных, с точки зрения использования памяти S-блоков подстановки, что необходимо для дальнейшего наращивания их длины, а также для использования в системах, которые имеют жесткие требования к аппаратным ресурсам, например, SMART-карты, а также для создания высокопроизводительных шифровальных систем, которые построены по принципу параллельных вычислений.

В смысле повышения эффективности существующих современных шифров, например, ГОСТ 28147-89 и Rijndael, и для разработки новых перспективных криптографических алгоритмов, задача синтеза нелинейных преобразований является ключевой и представляет наиболее существенный теоретический и практический интерес.

ГЛАВА 1
АНАЛИЗ СОВРЕМЕННЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ КРИПТОАЛГОРИТМОВ

В данной главе рассмотрены основные тенденции разработки криптографических примитивов современных блочных симметричных криптоалгоритмов на основе подхода, базирующегося на использовании математического аппарата булевых функций. Проведена классификация современных методов разработки S-блоков подстановки, используемых в современных шифрах.

Определены базовые критерии криптографического качества булевых функций, которые используются сегодня, и связь между ними, приводящая к существованию фундаментальных противоречий при разработке таких криптографических конструкций, как нелинейные преобразования современных шифров.

В свете понимания данных критериев приведены определения таких совершенных алгебраических конструкций как булевы бент-функции, которые играют значительную роль в современной криптографии.

1.1. Понятие S-блока подстановки и его назначение

Вопросы конструирования S-блоков подстановки с высокими криптографическими показателями качества интересуют специалистов-криптографов уже давно [1,2,3,4…11] и можно перечислить огромное число публикаций, посвященных этой проблеме. Наиболее последовательным является подход, основанный на алгебраических методах описания S-блоков подстановки с помощью аппарата булевых функций [12].

Анализ показывает, что, несмотря на хорошо проработанный математический аппарат, позволяющий выполнять строгое обоснование свойств, конструируемых S-блоков подстановки, предлагаемые современные подходы дают решения, ориентированные только на определенные классы шифров (например, DES-подобные), которые часто не лишены слабостей [13…16]. В этом свете, более прогрессивным подходом для построения S-блоков подстановки является разработка отдельных конструкций, таких как, например, конструкция, предложенная К. Ниберг [16].

Типичная конструкция S-блоков подстановки классических блочных криптографических алгоритмов (например, ГОСТ 28147-89) состоит из дешифратора, который преобразует k-разрядный двоичный сигнал в одноразрядный сигнал по модулю 2^k; системы внутренних связей (всего связей должно быть 2^k), и шифратора, который преобразует сигнал из одноразрядного 2^k-ичного в k-разрядный двоичный (рис.1.1) [17].

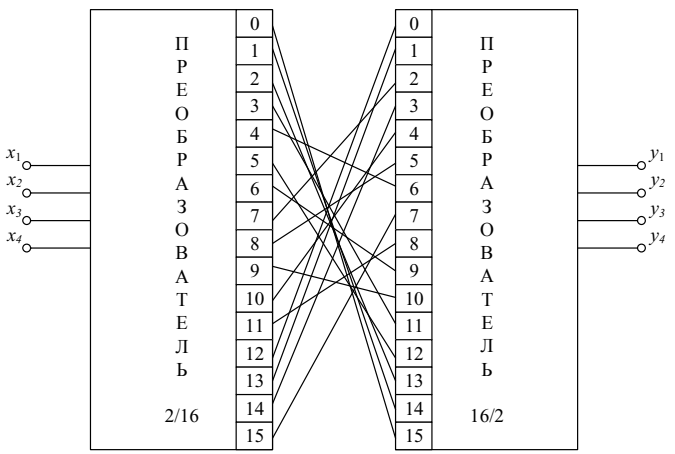


Рис. 1.1. Конструкция S-блока подстановки шифра ГОСТ 28147-89

Анализ рис. 1.1. показывает, что сущность преобразования, которое осуществляет S-блок подстановки можно пояснить как однозначное

соответствие между электродами дешифратора и электродами шифратора или соответствующими ячейками памяти, которые реализуют блок программно. Такое соответствие может быть представлено в виде соответствующего алгебраического выражения

$$S=\left\{\begin{array}{lcccccccccccccccc} X= & \{0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15\} \\ & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ Q= & \{15 & 14 & 13 & 11 & 6 & 12 & 9 & 2 & 5 & 10 & 4 & 8 & 0 & 1 & 3 & 7\} \end{array}\right\}, \quad (1.1)$$

где $X=[x_i]$, $i=\overline{1,2^k}$ — монотонно возрастающая последовательность натуральных чисел;

$Q=[y_j]$, $j=\overline{1,2^k}$ — кодирующая последовательность.

Q-последовательность — это многоуровневая числовая последовательность [3,4], которая построена из элементов последовательности X. Q-последовательность полностью определяет структуру и криптографические свойства S-блока подстановки, является первичным элементом его программной реализации.

Определение. S-блок подстановки называется биективным, если его Q-последовательность содержит все элементы последовательности X.

Проблема построения криптографических S-блоков подстановки по сути сводится к построению таких Q-последовательностей, которые бы удовлетворяли тому или иному критерию, выбранному при разработке S-блока подстановки [3].

Ясно, что полный код Q-последовательностей (общее количество всех существующих в природе Q-последовательностей) длины N состоит из $N!$ элементов. Таким образом, число различных структур Q-последовательностей стремительно растет с ростом длины N.

S-блок подстановки является нелинейным преобразованием, потому что для него в общем случае не выполняется принцип суперпозиции, который

можно сформулировать как равенство суммы преобразований пары исходных данных преобразованию суммы пары исходных данных $C = C'$

$$\begin{aligned} C &= Ta + Tb; \\ C' &= T(a + b), \end{aligned} \tag{1.2}$$

где T — преобразование S-блока подстановки.

Пусть $a = 1$, $b = 5$, тогда, учитывая (1.1) $Ta = 14$, а $Tb = 12$. Соответственно, выполняя сложение по модулю 2, получаем $Ta + Tb = 2$. С другой стороны $a + b = 4$, ведь $T(a + b) = 6$. Очевидно, что для нашего случая $C = 2 \neq C' = 6$, что доказывает факт нелинейности преобразования S-блока подстановки.

1.2. S-блоки подстановки современных криптографических алгоритмов и методы их построения

На сегодняшний день известно много подходов к построению Q-последовательностей. Из них можно выделить четыре главных:

— случайно выбрать. Ясно, что небольшие случайные S-блоки опасны, но большие случайно выбранные S-блоки могут оказаться довольно качественными [8]. Так, случайные S-блоки подстановки с восемью и больше входами уже довольно сильные. Например, в шифре IDEA [18] используются большие зависимые от ключа S-блоки подстановки;

— выбрать и проверить. Примеры такого подхода содержатся в [19, 20], где выбран подход к конструированию Q- последовательностей, когда они создаются согласно определенным критериям методом полного перебора. Такой подход довольно результативен, но вызывает трудности даже при длине Q-последовательности $N = 16$, потому что перебор всех 16! последовательностей может занимать большое время. Невозможно даже

представить, как этот метод можно адаптировать к S-блокам подстановки длины $N = 256$;

— разработать вручную. При этом математический аппарат используется крайне незначительно: S-блоки создаются с использованием интуитивных приемов;

— разработать математически. S-блоки создаются согласно математическим законам, поэтому они имеют гарантированную надежность по отношению к известным атакам криптоанализа, а также хорошими диффузными свойствами. Такой подход довольно распространен, примеры можно найти в [21…29].

Например, в соответствии с последним подходом, для построения S-блока подстановки шифра Rijndael/AES [30] разработчиками была выбрана конструкция Ниберг, которая представляет собой отображение, задаваемое мультипликативно обратными элементами поля Галуа $GF(2^k)$ [16]:

$$y = x^{-1} \bmod d[f(z), p], \quad y, x \in GF(2^k), \tag{1.3}$$

скомбинированное с аффинным преобразованием

$$b = A \cdot y + a, \quad a, b \in GF(2^k), \tag{1.4}$$

где $f(z) = z^8 + z^4 + z^2 + z + 1$ — несводимый над полем $GF(2)$ полином;

A — невырожденная матрица аффинного преобразования [31];

a — вектор сдвига;

$p = 2$ — характеристика расширенного поля Галуа, и принято, что $0^{-1} \equiv 0$;

a, b, x, y — элементы расширенного поля Галуа $GF(2^n)$, рассматриваются как десятичные числа, или двоичные векторы, или полиномы степени $k - 1$.

Важную задачу представляет измерение криптографического качества построенных S-блоков подстановки [32] — это основной вопрос независимо от того, какой способ построения S-блоков подстановки был выбран.

Для определения криптографического качества S-блоков подстановки целесообразно сначала представить полученный S-блок подстановки в виде его компонентных булевых функций F_i, $i=1,...,k$, как это показано в таблице 1.1. Для примера приведен S-блок подстановки длины $N=16$, который применяется в криптографическом алгоритме ГОСТ 28147-89 [33…37].

Таблица 1.1

Двоичное представление компонентных функций

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
x_2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
Q	15	14	13	11	6	12	9	2	5	10	4	8	0	1	3	7
F_1	1	0	1	1	0	0	1	0	1	0	0	0	0	1	1	1
F_2	1	1	0	1	1	0	0	1	0	1	0	0	0	0	1	1
F_3	1	1	1	0	1	1	0	0	1	0	1	0	0	0	0	1
F_4	1	1	1	1	0	1	1	0	0	1	0	1	0	0	0	0

Запишем каждую компонентную функцию в алгебраически-нормальной форме (АНФ) [12, 14, 38] с помощью многочленов Жегалкина, общий вид которых для случая 16-ты битных последовательностей

$$F_1(X=[x_1,x_2,x_3,x_4])=\sum_{i=0}^{15}a_iT_i=a_0T_0+a_1x_1+a_2x_2+$$
$$+a_3x_3+a_4x_4+a_5x_1x_2+a_6x_1x_3+a_7x_1x_4+a_8x_2x_3+a_9x_2x_4+a_{10}x_3x_4+ \quad (1.5)$$
$$+a_{11}x_1x_2x_3+a_{12}x_1x_2x_4+a_{13}x_1x_3x_4+a_{14}x_2x_3x_4+a_{15}x_1x_2x_3x_4,$$

где $a_i\in GF(2)$ — искомые коэффициенты, которые позволяют представить булеву функцию в АНФ. Находя эти коэффициенты и решая соответствующую систему уравнений, можно записать АНФ для каждой компонентной булевой функции из табл. 1.1.

$$\begin{cases} F_1(X) = 1 + x_1 + x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_2x_4 + x_1x_3x_4 + x_2x_3x_4; \\ F_2(X) = 1 + x_2 + x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_1x_2x_3 + x_2x_3x_4; \\ F_3(X) = 1 + x_1x_2 + x_1x_4 + x_2x_3 + x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4; \\ F_4(X) = 1 + x_3 + x_4 + x_1x_3 + x_1x_4 + x_2x_3 + x_3x_4 + x_2x_3x_4. \end{cases} \quad (1.6)$$

На этом этапе может быть определена алгебраическая степень нелинейности как минимальная среди максимальных степеней термов АНФ, то есть $\deg\{S\} = 3$. Количество термов в каждом уравнении системы (1.6) также является одним из показателей сложности функций [39], из которых состоит S-блок подстановки

$$\begin{cases} term(F_1) = 9; \\ term(F_2) = 9; \\ term(F_3) = 9; \\ term(F_3) = 8, \end{cases} \quad (1.7)$$

и также количества термов, которые включают определенную переменную

$$\begin{cases} term_{x_1}(F_1) = 4; \\ term_{x_2}(F_1) = 4; \\ term_{x_3}(F_1) = 5; \\ term_{x4}(F_1) = 3; \end{cases} \quad \begin{cases} term_{x_1}(F_3) = 5; \\ term_{x_2}(F_3) = 5; \\ term_{x_3}(F_3) = 5; \\ term_{x4}(F_3) = 5; \end{cases}$$

$$\begin{cases} term_{x_1}(F_2) = 4; \\ term_{x_2}(F_2) = 5; \\ term_{x_3}(F_2) = 3; \\ term_{x4}(F_2) = 4; \end{cases} \quad \begin{cases} term_{x_1}(F_2) = 2; \\ term_{x_2}(F_2) = 2; \\ term_{x_3}(F_2) = 5; \\ term_{x4}(F_2) = 4. \end{cases} \quad (1.8)$$

Определим другие важные показатели криптографического качества полученного S-блока подстановки.

1.3. Основные показатели криптографического качества S-блоков подстановки

1.3.1. Статистическая независимость выхода S-блока подстановки от его входа

Одним из наиболее распространенных критериев качества S-блоков подстановки заключается в том, что каждый бит исходного вектора y_j должен быть статистически независимым от каждого бита входного вектора x_i. Количественно степень линейной статистической (корреляционной) связи между выходными и входными битами описывается с помощью корреляционной матрицы $R = \left\| r_{i,j} \right\|$, $i, j = \overline{0, k-1}$, где $r_{i,j}$ — коэффициенты корреляции [40]

$$r_{i,j} = 1 - 2^{-(k-1)} \sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j}),\ i, j = \overline{0, k-1}. \tag{1.9}$$

Отсутствие корреляции между битами выхода и входа ($r_{i,j} = 0$) полагают хорошим качеством шифра [25], но исследователи все чаще склоняются к тому, что более оптимальным является равномерное распределение коэффициентов корреляции, то есть приблизительное равенство их абсолютных значений друг другу [15, 41].

Экстремальный случай, когда $r_{i,j} = 0$ при всех значения i и j возможен только тогда, когда каждая компонентная функция S-блока обладает корреляционным иммунитетом, по крайней мере, первого порядка [42…45].

Говорят, что функция f обладает корреляционным иммунитетом порядка p, если значение функции f статистически не зависит от любых p входных переменных [12, 19], то есть

$$\left\| \left\{ x' \in V_{k-p} : f^{a_1, a_2, \ldots, a_p}_{i_1, i_2, \ldots, i_p}(x') = 1 \right\} \right\| = 2^{k-p-1}, \tag{1.10}$$

где $f_{i_1,i_2,...,i_p}^{a_1,a_2,...,a_p}(x)$ — подфункции $f(x)$;

$i_1, i_2, ..., i_p$ — номера входных переменных, которые фиксируются;

$a_1, a_2, ..., a_p$ — значения, которые присваиваются соответствующим входным переменным.

В множестве 16-ти битных булевых функций существует 222 корреляционно иммунных функций (из них 212 имеют корреляционный иммунитет первого порядка, 8 — корреляционный иммунитет второго порядка, 2 — корреляционный иммунитет третьего порядка) [19].

Например, определим уровень корреляционного иммунитета для булевой функции, таблица истинности которой определяется как

$$f = \{0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0\} \qquad (1.11)$$

Построим таблицу, в которой найдем корреляционный иммунитет функции (1.11) во временной плоскости по определению (1.10).

Таблица 1.2

Пример нахождения корреляционного иммунитета

$\boldsymbol{x}_1$	x_2	x_3	x_4	$f'(x) = x_3 + x_4$	$f'(x) = x_3 + x_4$	x_1	$\boldsymbol{x}_2$	x_3	x_4
0	0	0	0	0	0	0	**0**	0	0
0	0	0	1	1	1	0	**0**	0	1
0	0	1	0	1	1	0	**0**	1	0
0	0	1	1	0	0	0	**0**	1	1
0	1	0	0	0	0	1	**0**	0	0
0	1	0	1	1	1	1	**0**	0	1
0	1	1	0	1	1	1	**0**	1	0
0	1	1	1	0	0	1	**0**	1	1
x_1	x_2	$\boldsymbol{x}_3$	x_4	$f'(x) = \mathrm{x}_4$	$f'(x) = \mathrm{x}_3$	x_1	x_2	x_3	$\boldsymbol{x}_4$
0	0	**0**	0	0	0	0	0	0	**0**
0	0	**0**	1	1	1	0	0	1	**0**
0	1	**0**	0	0	0	0	1	0	**0**
0	1	**0**	1	1	1	0	1	1	**0**
1	0	**0**	0	0	0	1	0	0	**0**
1	0	**0**	1	1	1	1	0	1	**0**
1	1	**0**	0	0	0	1	1	0	**0**
1	1	**0**	1	1	1	1	1	1	**0**

Требование корреляционного иммунитета определяет равенство количества значений $f'(x)=1$, принимаемых каждой подфункцией значению $2^{k-p-1}=2^{4-1-1}=2^2=4$ для корреляционного иммунитета первого порядка, которое равносильно требованию сбалансированности таблиц истинности каждой подфункции $f'(x)$, входящей в состав функции $f(x)$. Как видим, данное требование выполняется для вышеприведенного примера.

Для того, чтобы S-блок подстановки обладал корреляционным иммунитетом первого порядка, или, что равносильное, чтобы максимальный элемент матрицы коэффициентов корреляции равнялся нулю $\max\{R_{ij}\}=0$, необходимо, чтобы все компонентные функции данного S-блока владели корреляционным иммунитетом первого порядка [12].

Например, проведем расчеты матрицы коэффициентов корреляции S-блока подстановки (1.1)

$$R=\begin{pmatrix} \text{-0,2500} & \text{0,2500} & \text{0} & \text{0} \\ \text{0,2500} & \text{0} & \text{0} & \text{-0,2500} \\ \text{-0,2500} & \text{-0,2500} & \text{-0,2500} & \text{-0,2500} \\ \text{0,2500} & \text{0} & \text{-0,5000} & \text{-0,5000} \end{pmatrix}. \qquad (1.12)$$

Заметим, что корреляционное качество S-блоков подстановки удобно оценивать по абсолютному значению максимального коэффициента корреляции $R_{\max}=\max\{|R_{i,j}|\}$, которое для вышеупомянутого примера равняется $R_{\max}=0.5$.

1.3.2. Нелинейность S-блока подстановки

Другим важным критерием является максимизация расстояния нелинейности [46], которую можно определить как минимальное расстояние Хэмминга

$$N_f = \min(dist(F_i, A_j)), \quad i = \overline{1,k}, \quad j = 1, 2^{k+1}, \tag{1.13}$$

между компонентными функциями преобразования и всеми кодовыми словами аффинного $A(N,k)$-кода [12,38].

Для произвольного натурального k, аффинным $A(N,k)$-кодом длины $N = 2^k$ называется множество всех строк Ω_f тех булевых функций, степень нелинейности которых не превышает 1, то есть $A(N,k) = \{\Omega_f \mid f \in F_k, \deg f \le 1\}$ [12].

Таким образом, можно выписать все булевы функции степени $k = 4$, степень нелинейности которых не превышает 1.

$$\begin{cases} f_1(x_1,x_2,x_3,x_4) = 1; \\ f_2(x_1,x_2,x_3,x_4) = 1 \oplus x_1; \\ f_3(x_1,x_2,x_3,x_4) = 1 \oplus x_2; \\ f_4(x_1,x_2,x_3,x_4) = 1 \oplus x_3; \\ f_5(x_1,x_2,x_3,x_4) = 1 \oplus x_4; \\ f_6(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_2; \\ f_7(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_3; \\ f_8(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_4; \\ f_9(x_1,x_2,x_3,x_4) = 1 \oplus x_2 \oplus x_3; \\ f_{10}(x_1,x_2,x_3,x_4) = 1 \oplus x_2 \oplus x_4; \\ f_{11}(x_1,x_2,x_3,x_4) = 1 \oplus x_3 \oplus x_4; \\ f_{12}(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_2 \oplus x_3; \\ f_{13}(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_2 \oplus x_4; \\ f_{14}(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_3 \oplus x_4; \\ f_{15}(x_1,x_2,x_3,x_4) = 1 \oplus x_2 \oplus x_3 \oplus x_4; \\ f_{16}(x_1,x_2,x_3,x_4) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4; \end{cases} \quad \begin{cases} f_{17}(x_1,x_2,x_3,x_4) = 0; \\ f_{18}(x_1,x_2,x_3,x_4) = x_1; \\ f_{19}(x_1,x_2,x_3,x_4) = x_2; \\ f_{20}(x_1,x_2,x_3,x_4) = x_3; \\ f_{21}(x_1,x_2,x_3,x_4) = x_4; \\ f_{22}(x_1,x_2,x_3,x_4) = x_1 \oplus x_2; \\ f_{23}(x_1,x_2,x_3,x_4) = x_1 \oplus x_3; \\ f_{24}(x_1,x_2,x_3,x_4) = x_1 \oplus x_4; \\ f_{25}(x_1,x_2,x_3,x_4) = x_2 \oplus x_3; \\ f_{26}(x_1,x_2,x_3,x_4) = x_2 \oplus x_4; \\ f_{27}(x_1,x_2,x_3,x_4) = x_3 \oplus x_4; \\ f_{28}(x_1,x_2,x_3,x_4) = x_1 \oplus x_2 \oplus x_3; \\ f_{29}(x_1,x_2,x_3,x_4) = x_1 \oplus x_2 \oplus x_4; \\ f_{30}(x_1,x_2,x_3,x_4) = x_1 \oplus x_3 \oplus x_4; \\ f_{31}(x_1,x_2,x_3,x_4) = x_2 \oplus x_3 \oplus x_4; \\ f_{32}(x_1,x_2,x_3,x_4) = x_1 \oplus x_2 \oplus x_3 \oplus x_4. \end{cases} \tag{1.14}$$

Согласно построенным булевым функциям можно записать соответствующие таблицы истинности или кодовые слова аффинного кода, которые приведены в табл. 1.3.

Таблица 1.3

Кодовые слова аффинного кода, $k = 4$

F_i	Таблица истинности	Таблица истинности	F_i
F_1	1111111111111111	0000000000000000	F_{17}
F_2	1010101010101010	0101010101010101	F_{18}
F_3	1100110011001100	0011001100110011	F_{19}
F_4	1111000011110000	0000111100001111	F_{20}
F_5	1111111100000000	0000000011111111	F_{21}
F_6	1001100110011001	0110011001100110	F_{22}
F_7	1010010110100101	0101101001011010	F_{23}
F_8	1010101001010101	0101010110101010	F_{24}
F_9	1100001111000011	0011110000111100	F_{25}
F_{10}	1100110000110011	0011001111001100	F_{26}
F_{11}	1111000000001111	0000111111110000	F_{27}
F_{12}	1001011010010110	0110100101101001	F_{28}
F_{13}	1001100101100110	0110011010011001	F_{29}
F_{14}	1010010101011010	0101101010100101	F_{30}
F_{15}	1100001100111100	0011110011000011	F_{31}
F_{16}	1001011001101001	0110100110010110	F_{32}

Как видим, кодовые слова аффинного кода полностью совпадают с кодовыми словами кода Рида-Маллера первого порядка. Минимальное расстояние Хэмминга между кодовыми словами кода Рида-Маллера равняется $d_{\min} = 2^{k-1}$ [47]. Таким образом, для построенного выше аффинного кода минимальное расстояние Хэмминга определяется как $d_{\min} = 2^{k-1} = 2^3 = 8$.

Соответственно, расстояние нелинейности всего S-блока подстановки определяется как минимум среди всех расстояний нелинейности его компонентных функций

$$N_s = \min\{N_f\} = \min(dist(F_i, A_j)), \quad i = \overline{1,k}, \quad j = 1,2^{k+1}. \tag{1.15}$$

Известно [19,46], что для S-блоков подстановки, условием построения которых является сбалансированность компонентных булевых функций, расстояние нелинейности определяется как

$$N_{S\max} \le 2^{k-1} - 2^{(k/2)-1} - 2. \qquad (1.16)$$

Критерии оптимальной матрицы коэффициентов корреляции ($r_{i,j} = 0$) и высокого расстояния нелинейности S-блока подстановки являются несовместимыми, но, опираясь на высокую важность невозможности аппроксимации нелинейного преобразования аффинными функциями, все чаще разработчики шифров отдают предпочтение именно критерию равномерной минимизации элементов матрицы коэффициентов корреляции, что не исключает высокого расстояния нелинейности S-блока подстановки.

Преобразованием Уолша-Адамара булевой функции F от k переменных называется целочисленная функция, заданная на множестве Z_2^k двоичных векторов длины k равенством [48]

$$W_F(v) = \sum_{u \in Z_2^k} (-1)^{\langle u,v \rangle \oplus F(u)} \ . \qquad (1.17)$$

В литературе эту функцию также называют дискретным преобразованием Фурье или преобразованием Адамара функции. Значения $W_F(v)$ называются коэффициентами Уолша-Адамара функции. Для них справедливо равенство Парсеваля [48]:

$$\sum_{v \in Z_2^k} \left(W_F(v)\right)^2 = 2^{2k} \ . \qquad (1.18)$$

Поскольку число всех коэффициентов равняется 2^k, из равенства вытекает, что максимум модуля коэффициента Уолша–Адамара не может быть меньше величины $2^{k/2}$. Заметим, что расстояние Хэмминга от произвольной булевой функции до множества всех аффинных функций тесно связано с коэффициентами Уолша-Адамара этой функции. А именно, это расстояние равняется величине

$$N_f = 2^{k-1} - \frac{1}{2}\max_{v \in Z_2^k} \left| W_F(v) \right|. \quad (1.19)$$

Очевидно, что чем меньше максимум модуля коэффициентов Уолша-Адамара функции F, тем больше это расстояние.

В экстремальном случае, когда все коэффициенты преобразования Уолша-Адамара минимальны (это достигается только когда они равны по модулю), а расстояние нелинейности, соответственно, максимально, булева функция называется бент-функцией, а ее таблицы истинности, соответственно, бент-последовательностью [49].

Так, согласно определению [50] бинарная последовательность $B = [b_0, b_1, \cdots, b_i, \cdots, b_{n-1}]$, где $b_i \in \{\pm 1\}$ — коэффициенты, четной длины $N = 2^k$, $i = 0,1,...,k-1$, называется бент-последовательностью, если она имеет равномерный по модулю спектр Уолша-Адамара, который можно представить в матричной форме

$$W_B(\omega) = BA, \ \omega = 0,1,...,2^{k-1} \quad (1.20)$$

где A — матрица Уолша-Адамара порядка N [51].

Исходя из определения бент-функции, каждый спектральный коэффициент последовательности $W_B(\omega = 0), W_B(\omega = 1), ..., W_B(\omega = N-1)$ принимает значения из множества $\left\{\pm 2^{N/2}\right\}$.

Наиболее эффективным из известных методов построения бент-последовательностей длины N является конструкция Майорана-МакФарланда [52], которая основана на конкатенации строк матрицы Адамара A порядка $L = \sqrt{N} = 2^h$, а также всех возможных $L!$ перестановок ее строк и 2^L знаковых кодирований. Тогда как, в свою очередь, матрица Адамара A каждого следующего порядка строится соответственно с известным рекурентним правилом [53]

$$A_{2^h} = \begin{bmatrix} A_{2^{h-1}} & A_{2^{h-1}} \\ A_{2^{h-1}} & -A_{2^{h-1}} \end{bmatrix}, \tag{1.21}$$

где $A_1 = 1$.

Например , согласно (1.21) построим матрицу Адамара A_8 (где для краткости $+1$ обозначенны как "+ ", а -1 как "– ")

$$\mathbf{A}_8 = \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & + & + & - & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & + & - & - & + & - & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & - & + & + & - \end{bmatrix}, \tag{1.22}$$

и, применяя последовательную конкатенацию ее строк, получаем бент-последовательность длины $N = 64$ и согласно (1.20) ее спектр Уолша-Адамара

$$\begin{aligned} \mathbf{B} = [&+ + + + + + + + + - + - + - + - + + - - + + - - + - + + - - + \\ &+ + + + - - - - + - + - - + - + + + - - - - + + + - - + - + + + -] \\ \mathbf{F}(\omega) = [&8\ 8\ 8\ 8\ 8\ 8\ 8\ 8\ 8\ 8\ -8\ 8\ -8\ 8\ -8\ 8\ 8\ -8\ 8\ 8\ -8\ -8\ 8\ 8 \\ &-8\ -8\ 8\ -8\ -8\ -8\ 8\ 8\ -8\ -8\ 8\ -8\ 8\ 8\ 8\ -8\ -8\ 8\ -8\ -8\ 8\ -8\ 8 \\ &-8\ -8\ 8\ -8\ 8\ 8\ 8\ -8\ -8\ -8\ -8\ 8\ 8\ 8\ -8\ -8\ 8\ -8\ 8\ 8\ -8], \end{aligned} \tag{1.23}$$

то есть последовательность (1.23) действительно удовлетворяет определению бент-последовательности.

В настоящее время теория бент-функций довольно развита, но основная задача — синтез полных классов бент-функций произвольной длины N остается нерешенной, хотя и существуют методы, позволяющие получить некоторые элементы этого множества [54-58].

1.3.3. Период возврата S-блока подстановки в исходное состояние

Следующий критерий криптографического качества S-блоков подстановки — периоды возврата S-блока подстановки в исходное состояние определяются как число итераций до возвращения S-блока подстановки в

начальное состояние при продолжительном входном воздействие [59…60]. Найдем период возврата для приведенного выше примера (1.1), подав на его вход тривиальное воздействие и отследив поведение подстановочной конструкции при зацикливании её выхода на вход

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & \rightarrow \\ 15 & 14 & 13 & 11 & 6 & 12 & 9 & 2 & 5 & 10 & 4 & 8 & 0 & 1 & 3 & 7 & \rightarrow \\ 7 & 3 & 1 & 8 & 9 & 0 & 10 & 13 & 12 & 4 & 6 & 5 & 15 & 14 & 11 & 2 & \rightarrow \\ 2 & 11 & 14 & 5 & 10 & 15 & 4 & 1 & 0 & 6 & 9 & 12 & 7 & 3 & 8 & 13 & \rightarrow \\ 13 & 8 & 3 & 12 & 4 & 7 & 6 & 14 & 15 & 9 & 10 & 0 & 2 & 11 & 5 & 1 & \rightarrow \\ 1 & 5 & 11 & 0 & 6 & 2 & 9 & 3 & 7 & 10 & 4 & 15 & 13 & 8 & 12 & 14 & \rightarrow \\ 14 & 12 & 8 & 15 & 9 & 13 & 10 & 11 & 2 & 4 & 6 & 7 & 1 & 5 & 0 & 3 & \rightarrow \\ 3 & 0 & 5 & 7 & 10 & 1 & 4 & 8 & 13 & 6 & 9 & 2 & 14 & 12 & 15 & 11 & \rightarrow \\ 11 & 15 & 12 & 2 & 4 & 14 & 6 & 5 & 1 & 9 & 10 & 13 & 3 & 0 & 7 & 8 & \rightarrow \\ 8 & 7 & 0 & 13 & 6 & 3 & 9 & 12 & 14 & 10 & 4 & 1 & 11 & 15 & 2 & 5 & \rightarrow \\ 5 & 2 & 15 & 1 & 9 & 11 & 10 & 0 & 3 & 4 & 6 & 14 & 8 & 7 & 13 & 12 & \rightarrow \\ 12 & 13 & 7 & 14 & 10 & 8 & 4 & 15 & 11 & 6 & 9 & 3 & 5 & 2 & 1 & 0 & \rightarrow \end{bmatrix}$$
$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \end{bmatrix}. \qquad (1.29)$$

Как видим, S-блок подстановки возвращается в исходное состояние, равное тривиальному воздействию после $T = 12$ периодов, что определяет величину его периода возврата.

Иной способ нахождения периода возврата S-блока в исходное состояние состоит в нахождении полного разложения S-блока подстановки на циклы:

$$Q = \{C_{12}(15,7,2,13,1,14,3,11,8,5,12,0),\ C_4(6,9,10,4)\}, \qquad (1.30)$$

где индексы определяют длину цикла, а значения в круглых скобках — элементы S-блока из данного цикла. Криптографическая стойкость блока подстановки в целом будет определяться как

$$T = HOK(i_1, i_2 ...), \qquad (1.31)$$

где i — соответствующие длины циклов. В нашем случае, нетрудно видеть, что $T = 12$.

1.3.4 Строгий лавинный критерий

Строгий лавинный критерий можно неформально определить как равную вероятность изменения каждого выходного бита при изменении одного входного бита S-блока подстановки [12, 19, 61…62].

Известный американский ученный К. Э. Шеннон ввел понятия конфузии и диффузии в качестве методов, которые усложняют криптоанализ. Согласно Шеннону [48]:

Диффузия — метод, при котором избыточность в статистике входных данных "распределяется" по всей структуре выходных данных. При этом для статистического анализа нужны большие объемы входных данных. Диффузия приводит к скрытию структуры открытого текста. Реализуется с помощью P-блоков.

Конфузия — метод, при котором зависимость ключа и выходных данных делается, по возможности, более сложной, в частности, нелинейной. При этом криптоаналитику становится сложнее строить предположения о структуре ключа по входным данным, а также об выходных данных, если известна часть ключа. Метод конфузии реализуется с помощью S-блоков постановки.

Лавинный эффект является следствием хорошей конфузии и диффузии. Количественно лавинный критерий возможно определить через коэффициент распространения ошибки как

$$K_i(f) = \sum_{a_i} \big(f(x) \oplus f(x \oplus e_i) \big) = 2^{\eta-1}, \tag{1.32}$$

где η — размерность компонентной функции S-блока подстановки.

Для S-блоков постановки обычно строятся таблицы весов производных для каждой компонентной булевой функции исходя из (1.32). Так, для нашего примера (1.1) можем найти таблицу весов производных компонентных булевых функций.

Таблица 1.4.

Веса производных компонентных булевых функций

e_i	$\sum_{a_i}(f_1(x)\oplus f_1(x\oplus e_i))$	$\sum_{a_i}(f_2(x)\oplus f_2(x\oplus e_i))$	$\sum_{a_i}(f_3(x)\oplus f_3(x\oplus e_i))$	$\sum_{a_i}(f_4(x)\oplus f_4(x\oplus e_i))$
0001	8	8	8	8
0010	8	12	8	4
0100	12	8	8	8
1000	8	8	8	8

Анализ данных табл. 1.4. показывает, что только компонентные булевы функции f_1 и f_4 соответствуют условию (1.32), т.е. удовлетворяют строгому лавинному критерию, а, стало быть, S-блок подстановки (1.1) в целом строгому лавинному критерию не удовлетворяет.

1.4. Обобщения и открытые проблемы

Опираясь на обзор современных методов построения криптографических S-блоков подстановки и критериев, которые к ним предъявляются, можем привести классификационную схему (рис 1.2) известных методов построения S-блоков подстановки, которые отвечают базовым критериям качества.

Следует отметить, что многие методы, приведенные на рис. 1.2, позволяют синтезировать S-блоки подстановки, которые могут также иметь удовлетворительные показатели криптографического качества и согласно другим критериям, но в приведенной схеме они сгруппированы согласно приоритетному критерию, то есть такому, на который обращено внимание разработчиков в первую очередь.

Несмотря на то, что за последние десятилетия сложилась, можно сказать, теория синтеза криптографических S-блоков подстановки, многие проблемы остаются открытыми и мало исследованными.

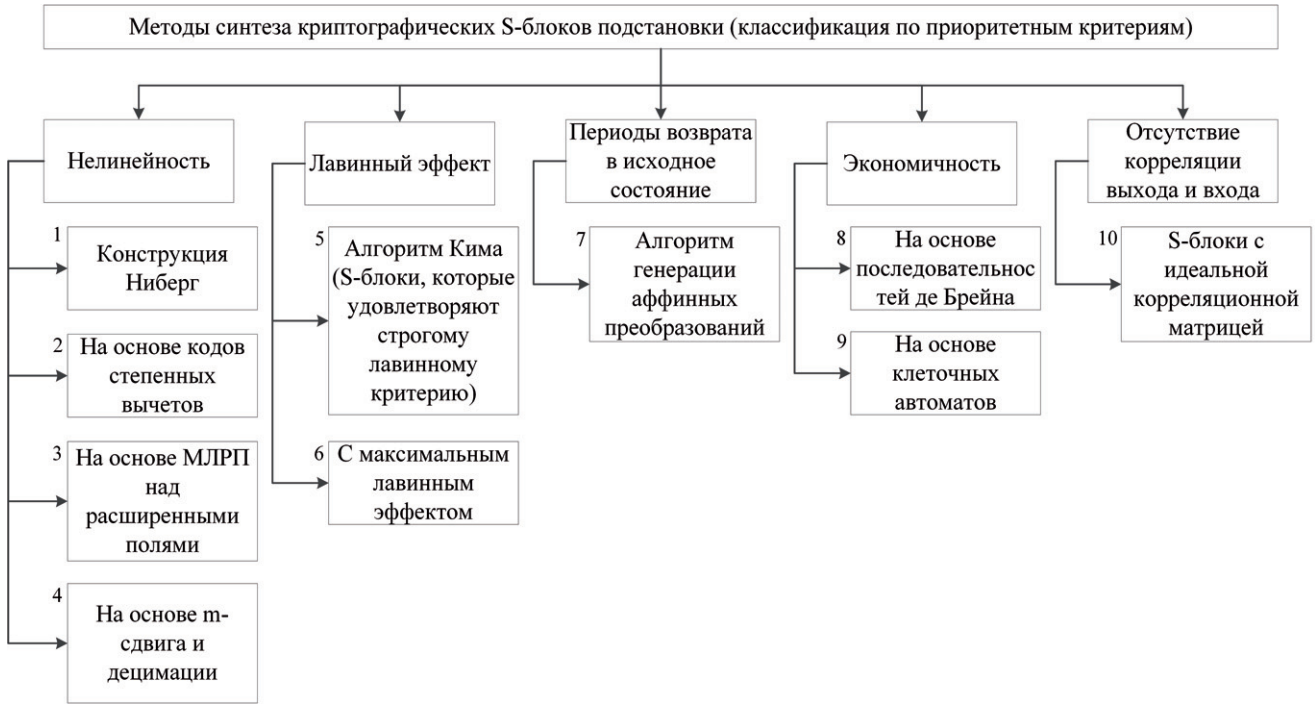


Рис. 1.2. Классификационная схема методов синтеза *S*-блоков подстановки

Так, в работе [48] показано, что качество криптографических S-блоков подстановки значительно улучшается с ростом их длины N, что ведет к стремительному росту криптостойкости шифров, в которых они применяются. В настоящее время в литературе мало освещены эффективные методы синтеза S-блоков подстановки длины $N > 2^k = 2^8$, то есть более чем однобайтные. Не существует эффективных с вычислительной точки зрения методов оценки параметров многобайтных подстановок. Так, например, для оценки нелинейности S-блока подстановки длины $N = 2^{3\cdot8} = 2^{24}$ будет необходимо сгенерировать аффинный код, представляющий собой матрицу размера $2^{25} \times 2^{24}$, для хранения которой придется выделить приблизительно 64 терабайта памяти. Также непростой будет реализация таких S-блоков подстановки. В этом смысле, наверное, наилучшим решением может стать применение математического аппарата клеточных автоматов. Однако, проблемы конструирования S-блоков подстановки на основе клеточных автоматов, которые предложены к использованию в [63], остаются фактически нерешенными. Неизвестны оптимальные структуры правил эволюции, которые управляют клеточными автоматами, приводящие к формированию оптимальных S-блоков подстановки. Неизвестны даже регулярные методы синтеза правил, которые приводят к формированию биективных S-блоков подстановки.

Важной проблемой является также изучение таких критериев как алгебраическая степень нелинейности S-блоков подстановки, аффинная независимость их компонентных булевых функций [64]. Эти вопросы также остаются нерешенными.

Очень интересными являются вопросы построения рекуррентных алгоритмов конструирования S-блоков подстановки, которые обладают заданным уровнем криптографической стойкости. Такие алгоритмы открывают путь к конструированию сколь угодно больших S-блоков подстановки по

относительно несложным алгоритмам, что является очень ценной возможностью получения таких конструкций.

И, конечно, такая проблема математики и теории передачи информации, как синтез совершенных алгебраических конструкций неразрывно связанна с проблемами теории синтеза S-блоков подстановки. Такими перспективными конструкциями могут быть такие двоичные и многоуровневые последовательности:

1. бент-функции, или бент-последовательности [49…50, 54…57, 65…66];
2. совершенные двоичные решетки [67…69];
3. последовательности де Брейна [11, 70…72];
4. конструкции полей Галуа: МЛРП, m-последовательности, коды степенных вычетов, и т.п. [73…75];
5. торы де Брейна [76…78].

Разработка новых алгоритмов синтеза вышеприведенных алгебраических конструкций будет приводить к появлению новых, более эффективных методов синтеза высококачественных S-блоков подстановки.

ГЛАВА 2
МЕТОДЫ СИНТЕЗА S-БЛОКОВ ПОДСТАНОВКИ, СООТВЕТСТВУЮЩИХ СТРОГОМУ ЛАВИННОМУ КРИТЕРИЮ

2.1. Методы синтеза S-блоков подстановки, соответствующих лавинному критерию на основе бент-функций

В последнее время исследователями довольно много внимания уделяется конструированию S-блоков подстановки, удовлетворяющих критериям высокой нелинейности, а также S-блоков подстановки, которые удовлетворяют строгому лавинному критерию [7, 16], в то время как вопрос построения S-блоков подстановки, удовлетворяющих одновременно двум критериям также является достаточно актуальным для современного состояния развития криптографии. Данный вопрос может быть решен, как показали исследования, благодаря таким совершенным алгебраическим конструкциям, как бент-функции. Акцент в имеющихся разработках, в условиях постоянного роста длины S-блока подстановки $N = 2^k$, делается на создании регулярных методов их синтеза без применения полного перебора.

Как было показано в предыдущих главах, одной из конструкций, которая представляет регулярный метод синтеза высоконелинейных S-блоков подстановки является конструкция Ниберг [41], применяемая в криптопреобразовании Rijndael/AES. S-блоки подстановки, построенные по правилам данной конструкции, достигают практически максимального значения расстояния нелинейности $N_s = 112$ [41]. Однако, оказывается, что они не отвечают строгому лавинному критерию [15].

Попытка создания конструктивных методов синтеза S-блоков подстановки, которые бы отвечали строгому лавинному критерию была

предпринята в [24]. Однако, эти S-блоки подстановки не удовлетворяют критерию высокой нелинейности.

Основные материалы по разработанному новому методу изложены в [10].

Для полноты изложения материала приведем сущность рекуррентного алгоритма построения S-блоков подстановки, которые отвечают строгому лавинному критерию [24], иллюстрируя его конкретным примером:

Алгоритм А1:

Шаг 1. Переборным методом проводится построение S-блоков подстановки малой длины, которые удовлетворяют строгому лавинному критерию. Например, для длины входного блока $k = 3$, такая задача не представляет трудностей, поскольку объем полного множества таких S-блоков подстановки составляет всего $J = 2^k ! = 8! = 40320$. Установлено, что для данной длины существует $V = 4608$ S-блоков подстановки, которые удовлетворяют строгому лавинному критерию. Из данного множества, выберем, например, S-блок подстановки

$$Q = \{4\ 7\ 2\ 6\ 1\ 5\ 0\ 3\}, \tag{2.1}$$

обозначив его $S_k = S_3 = Q$.

Шаг 2. Задаем функцию F_m, как MSB (старшие значащие биты) выбранного на шаге 1 S-блока подстановки S_k. В нашем случае, очевидно

$$F_m = F_2 = \{1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\}. \tag{2.2}$$

Шаг 3. Производим удвоение длины функции F_m по правилу горизонтальной конкатенации

$$G_1[F_m] = \left\{F_m(x) \,|\, F_m\left(x \oplus e_k^{(\alpha)}\right) \oplus 1\right\},\ x = 0,1,...,2^k - 1 \tag{2.3}$$

где $e_k^{(\alpha)}$ — вектор длины k, который содержит 1 на позиции α;

"|" — символ горизонтальной конкатенации.

Например, выберем $e_k^{(\alpha)} = \{1\ 0\ 0\}$, тогда

$$G_1[F_m]=\{0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 0\ 0\}. \quad (2.4)$$

Шаг 4. Удваиваем длину S-блока подстановки S_k по правилу

$$G_0[S_{k+1}]=\{S_k(x)\,|\,S_k(x\oplus e_t)\},\ x=0,1,...,2^k-1. \quad (2.5)$$

Для нашего примера, снова выбирая $e_k^{(\alpha)}=\{1\ 0\ 0\}$, получаем новый небиективный S-блок подстановки (то есть такой, Q-последовательность которого содержит одинаковые элементы)

$$G_0[S_3]=\{4\ 7\ 2\ 6\ 1\ 5\ 0\ 3\ 7\ 4\ 6\ 2\ 5\ 1\ 3\ 0\}. \quad (2.6)$$

Шаг 5. Строим новый биективный S-блок подстановки $S_{k+1}=S_4$ удвоенной длины $N=2^{k+1}=16$, который также удовлетворяет строгому лавинному критерию по правилу

$$S_{k+1}=\{G_1[F_m]\cdot 2^k+G_0[S_k]\}. \quad (2.7)$$

Используя полученные ранее функции $G_1[F_m]$ и $G_0[S_k]$ получаем S-блок подстановки

$$S_4=\{4\ 7\ 2\ 14\ 1\ 13\ 8\ 11\ 15\ 12\ 6\ 10\ 5\ 9\ 3\ 0\} \quad (2.8)$$

Построив таблицу весов производных компонентных булевых функций $wt(D_{i,k})$ для нового S-блока подстановки (2.80) удвоенной длины, также получаем, что он удовлетворяет строгому лавинному критерию

Таблица 2.1

Таблица весов производных компонентных булевых функций

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$
0001	8	8	8	8
0010	8	8	8	8
0100	8	8	8	8
1000	8	8	8	8

Шаг 6. Возвращаемся к шагу 2 и повторяем алгоритм до тех пор, пока не будет достигнута необходимая длина S-блока подстановки $N = 2^k$.

Например, повторив вышеприведенный алгоритм 5 раз, получаем S-блок подстановки S_8 длины $N = 2^8 = 256$, который может использоваться в криптоалгоритме Rijndael/AES

Таблица 2.2

S-блок подстановки S_8 длины $N = 2^8 = 256$

S_8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	54	57	02	FE	01	FD	A8	AB	AF	AC	06	FA	05	F9	53	50
1	A7	A4	0E	F2	0D	F1	5B	58	5C	5F	0A	F6	09	F5	A0	A3
2	B7	B4	1E	E2	1D	E1	4B	48	4C	4F	1A	E6	19	E5	B0	B3
3	44	47	12	EE	11	ED	B8	BB	BF	BC	16	EA	15	E9	43	40
4	97	94	3E	C2	3D	C1	6B	68	6C	6F	3A	C6	39	C5	90	93
5	64	67	32	CE	31	CD	98	9B	9F	9C	36	CA	35	C9	63	60
6	74	77	22	DE	21	DD	88	8B	8F	8C	26	DA	25	D9	73	70
7	87	84	2E	D2	2D	D1	7B	78	7C	7F	2A	D6	29	D5	80	83
8	D7	D4	7E	82	7D	81	2B	28	2C	2F	7A	86	79	85	D0	D3
9	24	27	72	8E	71	8D	D8	DB	DF	DC	76	8A	75	89	23	20
A	34	37	62	9E	61	9D	C8	CB	CF	CC	66	9A	65	99	33	30
B	C7	C4	6E	92	6D	91	3B	38	3C	3F	6A	96	69	95	C0	C3
C	14	17	42	BE	41	BD	E8	EB	EF	EC	46	BA	45	B9	13	10
D	E7	E4	4E	B2	4D	B1	1B	18	1C	1F	4A	B6	49	B5	E0	E3
E	F7	F4	5E	A2	5D	A1	0B	08	0C	0F	5A	A6	59	A5	F0	F3
F	04	07	52	AE	51	AD	F8	FB	FF	FC	56	AA	55	A9	03	00

Таблица весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$ для S-блока подстановки (табл. 2.2) также состоит из элементов равных 2^{k-1}, что говорит о том, что данный S-блок подстановки удовлетворяет строгому лавинному критерию

Исследования свойств нелинейности S-блока подстановки (табл. 2.3) показали, что его расстояние нелинейности равняется $N_s = 64$, что существенно меньше 112, при этом алгебраическая степень нелинейности $\deg\left(S_8\right) = 2$.

Таблица 2.3

Таблица весов производных компонентных булевых функций

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
10000000	128	128	128	128	128	128	128	128
01000000	128	128	128	128	128	128	128	128
00100000	128	128	128	128	128	128	128	128
00010000	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00000010	128	128	128	128	128	128	128	128
00000001	128	128	128	128	128	128	128	128

Рассмотрим возможность устранения данного недостатка, для чего более подробно изучим сущность вышеприведенного алгоритма рекуррентного увеличения длины N S-блока подстановки. Тщательный анализ данного алгоритма показывает, что по сути каждая его итерация является модификацией конструкции, показанной на рис. 2.2, которая была изучена в [23].

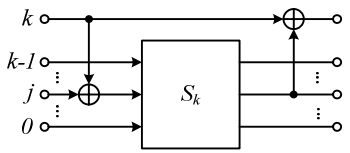


Рис. 2.1. Рекурентная схема увеличения длины S-блока подстановки

Очевидно, низкая нелинейность S-блока подстановки (табл. 2.2) вытекает из недостаточно сложного закона формирования k-го выхода S-блока подстановки (рис. 2.1). Такое обстоятельство приводит к тому, что на каждой следующей итерации увеличения размера S-блока подстановки его нелинейность возрастает непропорционально росту длины N, что ведет к неминуемой деградации данного параметра.

Ключ к устранению указанного недостатка лежит в замене схемы, изображенной на рис. 2.1 на более сложную схему [23], изображенную на рис.

2.2, в которой применяется дополнительная булева функция g от k переменных, свойства которой определяют сложность k-й компонентной булевой функции нового S-блока подстановки удвоенной длины.

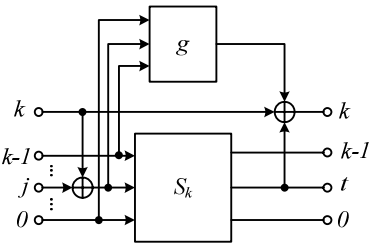


Рис. 2.2. Рекурентная схема увеличения длины S-блока подстановки, со сложным алгоритмом формирования дополнительной булевой функции

Анализ работы схемы (рис. 2.2) показывает, что задача проектирования свойств S-блоков подстановки, которые создаются, может быть сведена к задаче проектирования свойств исходного S-блока подстановки S_k, а также свойств булевой функции g, применяемой на каждой итерации.

Проведенные исследования показывают, что для построения S-блоков подстановки, которые одновременно удовлетворяют критериям высокой нелинейности и строгому лавинному критерию, в качестве исходных S-блоков подстановки необходимо выбрать такие, которые удовлетворяют строгому лавинному критерию (для малых значений k они могут быть легко найдены с помощью метода полного перебора), а в качестве функции g, длина которой на каждой итерации соответственно будет равна 2^k, необходимо использовать SAC булевы функции с максимальным расстоянием нелинейности, для четных k, соответственно, известные в литературе как бент-функции [65].

Для значений $k=\{4,16,64,256...\}$, для которых $\kappa=\sqrt{k}$ — целое число, построение необходимых для алгоритма (рис. 2.2) бент-функций возможно с помощью конструкции Майорана МакФарланда [51] путем конкатенации строк

матрицы Адамара $H(\kappa)$ и их любых знаковых кодирований Z и перестановок P. Всего возможно построить $|Z|\cdot|P| = 2^k \cdot k!$ таких бент-функций. Опытным путем установлено, что все они удовлетворяют строгому лавинному критерию.

Для итераций алгоритма на которых $k \neq \kappa$ необходимо воспользоваться следующим экспериментально установленным утверждением:

Утверждение. На периоде бент-функции Майорана-МакФарланда длины $N = 2^\kappa$ всегда существует хотя бы один сегмент длины $\lambda = 2^k, 2 \le k \le \kappa$ удовлетворяющий строгому лавинному критерию.

Таким образом, мы можем записать метод построения криптографических S-блоков подстановки, которые удовлетворяют одновременно двум упомянутым критериям в виде следующих шагов, проиллюстрированных примером:

Шаг 1. Выбираем необходимый размер S-блоков подстановки $N_\tau = 2^{k_\tau}$ и исходный размер $N_u = 2^{k_u} \le N_\tau$, где индексы τ и u означают необходимый и исходный S-блок подстановки соответственно. Методом перебора находим все S-блоки размера N_u, которые удовлетворяют строгому лавинному критерию.

Например, пусть $N_\tau = 2^{k_\tau} = 2^8 = 256$, а исходный S-блок подстановки длины $N_u = 2^{k_u} = 2^3 = 8$ определяется как (2.1), то есть $S_3 = Q$.

Шаг 2. Строим булеву функцию g как двоичное отображение бент-последовательности, построенной по правилу Майорана-МакФарланда с параметрами перестановки P и знакового кодирования Z и с учетом Утверждения. Для нашего примера в качестве такой бент-функции можно избрать $g = \{0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\}$.

Шаг 3. Используя схему, приведенную на рис. 2.2 удваиваем размер S-блока подстановки N. Если достигнут размер $N = N_\tau$ переходим к шагу 4, иначе, возвращаемся на шаг 2. В нашем примере для достижения величины $N_\tau = 256$ потребуется сделать 5 итераций.

Шаг 4. Установлено, что имеет место ситуация, когда нелинейность распределена по компонентным булевым функциям неравномерно, что ведет к снижению общей нелинейности S-блока. Для устранения неравномерного распределения нелинейности по компонентным булевым функциям построенного S-блока длины $N_\tau = 2^8 = 256$ применим следующий алгоритм:

а) просуммируем первую половину компонентных булевых функций по правилу

$$F_i = F_i \oplus F_6, i = 0,1,...,3\ , \tag{2.9}$$

б) просуммируем вторую половину компонентных булевых функций по правилу

$$F_i = F_i \oplus F_3 \oplus F_7,\ i = 4,5\,. \tag{2.10}$$

Пример применения описанного выше алгоритма для исходного S-блока подстановки (2.1), и правил знакового кодирования $Z = \{1,1,...,1\}$ и перестановки $P = \{1,2,...,2^\kappa\}$, примененных на каждой итерации, которая позволяет построить S-блок подстановки заданной длины $N_\tau = 256$ приведенный в табл. 2.4.

Таблица 2.4.

S-блок подстановки S_8 длины $N = 2^8 = 256$, созданный новым алгоритмом

S_8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	04	3F	1A	26	89	9D	A8	BB	01	5A	30	6C	8C	F8	82	F1
1	11	A5	7F	CC	BC	27	ED	71	14	C0	55	86	B9	42	C7	3B
2	31	35	90	93	E3	C8	7D	51	34	50	BA	D9	E6	AD	57	1B
3	24	AF	F5	79	D6	72	38	9B	21	CA	DF	33	D3	17	12	D1
4	4E	4A	5F	5C	2C	07	02	2E	FB	9F	C5	A6	99	D2	98	D4
5	5B	D0	3A	B6	19	BD	47	E4	EE	05	A0	4C	AC	68	DD	1E
6	7B	40	D5	E9	46	52	D7	C4	CE	95	4F	13	F3	87	4D	3E
7	6E	DA	B0	03	73	E8	92	0E	DB	0F	2A	F9	C6	3D	08	F4
8	FE	FA	EF	EC	9C	B7	B2	9E	4B	2F	75	16	29	62	28	64
9	EB	60	8A	06	A9	0D	F7	54	5E	B5	10	FC	1C	D8	6D	AE
A	CB	F0	65	59	F6	E2	67	74	7E	25	FF	A3	43	37	FD	8E
B	DE	6A	00	B3	C3	58	22	BE	6B	BF	9A	49	76	8D	B8	44
C	B4	8F	AA	96	39	2D	18	0B	B1	EA	80	DC	3C	48	32	41
D	A1	15	CF	7C	0C	97	5D	C1	A4	70	E5	36	09	F2	77	8B
E	81	85	20	23	53	78	CD	E1	84	E0	0A	69	56	1D	E7	AB
F	94	1F	45	C9	66	C2	88	2B	91	7A	6F	83	63	A7	A2	61

S-блок подстановки (табл. 2.4) имеет таблицу весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$

Таблица 2.5

Таблица весов производных компонентных булевых функций

e_j	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	128	128	128	128	128	128	128	128
01000000	128	128	128	128	128	128	128	128
00100000	128	128	128	128	128	128	128	128
00010000	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00000010	128	128	128	128	128	128	128	128
00000001	128	128	128	128	128	128	128	128

Указанный S-блок подстановки (табл. 2.4) обладает расстоянием нелинейности $N_s = 112$ и превосходит по криптографическим свойствам S-блоки подстановки конструкции Ниберг, применяемой в криптоалгоритме Rijndael/AES.

Найдем количество разных структур S-блоков подстановки, которые могут быть построены с помощью предложенного метода. Пусть $k_u = 3$, тогда количество исходных S-блоков подстановки, которые удовлетворяют строгому лавинному критерию $V = 4608$, а количество бент-функций Майорана МакФарланда $W_3 = |P||Z| = 2^4 \cdot 4! = 384$. Итого, пройдя первую итерацию мы можем построить $J_1 = 384 \cdot 4608 = 1769472$ оптимальных S-блоков подстановки. На второй итерации, из полученных S-блоков подстановки можно построить в $W = |P||Z| = 2^4 \cdot 4! = 384$ раза большее количество S-блоков подстановки, то есть $J_2 = 384 \cdot 1769472 = 679477248$. Итого, можем записать формулу мощности класса оптимальных S-блоков подстановки для k_τ-и итерации

$$J_{k_\tau} = V \cdot \prod_{k=k_u}^{k_\tau - 1} W_k . \qquad (2.11)$$

Таким образом, согласно выражению (2.11) для $k_u = 3$, и для $k_\tau = 8$ можно построить $J_8 = (2^4 \cdot 4!) \cdot (2^4 \cdot 4!) \cdot (2^6 \cdot 6!) \cdot (2^6 \cdot 6!) \cdot (2^8 \cdot 8!) \approx 3.23 \cdot 10^{21}$ оптимальных S-блоков подстановки.

Отметим, что полученные S-блоки подстановки имеют довольно низкие максимумы матриц коэффициентов корреляции R, при этом алгебраическая степень нелинейности сохраняется на уровне $\deg(S) = 2$, что продиктовано соответствием строгому лавинному критерию.

Нетрудно видеть операции, с помощью которых может быть произведено размножение оптимальных S-блоков подстановки при сохранении их соответствия строгому лавинному критерию и критерию высокой нелинейности. Так, путем изменения порядка следования компонентных булевых функций, а также всех возможных их знаковых кодирований из одного построенного по предложенному методу S-блока подстановки, могут быть построены новые $2^{k_\tau} \cdot k_\tau!$ S-блоков подстановки, большинство из которых будут также принадлежать к рассчитанному числу (2.11). Также новые S-блоки подстановки могут быть получены с помощью m-сдвигов [3] исходного S-блока подстановки на величину $\upsilon = 0,1,..,2^{k_\tau} - 1$.

2.2. Метод синтеза корреляционно иммунных S-блоков подстановки, удовлетворяющих строгому лавинному критерию

Помимо построения высоконелинейных S-блоков подстановки, удовлетворяющих строгому лавинному критерию актуальной задачей является построение S-блоков подстановки, соответствующих одновременно строгому лавинному критерию и критерию корреляционного иммунитета. Имеется алгоритм синтеза S-блоков подстановки, соответствующих строгому лавинному критерию [24]. С другой стороны также известен алгоритм построения оптимальных S-блоков подстановки, которые удовлетворяют критерию нулевой

корреляции между векторами выхода и входа S-блока подстановки, т.е. являются корреляционно иммунными.

Отметим, что раньше в [6] имела место попытка синтеза S-блоков подстановки длины $N=16$, которые удовлетворяют как строгому лавинному критерию, так и критерию нулевой корреляции между векторами выхода и входа S-блока подстановки, в результате чего переборным методом было показано, что несмотря на то, что существуют 24 булевы функции, которые удовлетворяют этим критериям, на их основе не может быть построен ни один криптографический S-блок подстановки, который удовлетворяет одновременно строгому лавинному критерию и критерию нулевой корреляции между векторами выхода и входа одновременно.

Основные результаты исследований приведены в работе [79]. Так, был проведен поиск булевых функций, которые удовлетворяют одновременно строгому лавинному критерию и критерию нулевой корреляции между векторами выхода и входа S-блока подстановки длины $N=32$, в результате чего было найдено множество Ψ из 7080 сбалансированных булевых функций. Отметим, что среди данных функций нет ни одной, которая бы имела корреляционный иммунитет $m>1$ порядка.

Построение S-блоков подстановки на основе найденных функций переборным методом требует около $C_{7080}^{5}=1{,}48\cdot 10^{17}$ итераций, что является довольно затруднительным с точки зрения технической реализации. Отметим, что в [80] разработан эффективный алгоритм синтеза криптографических S-блоков подстановки на основе заданного множества булевых функций, в основу которого положено предположения о том, что криптографический биективный S-блок подстановки может быть построен только на основе таких k булевых функций для которых все линейные комбинации являются сбалансированными, то есть

$$wt\left(\sum_{z=1}^{k} a_z \cdot \Phi_z\right) = 2^{k-1}, z=\overline{1,k}\ , \qquad (2.12)$$

для любых $a_z \in \{0,1\}$, $\{a_1, a_2, ..., a_k\} \neq \{0,0,...0\}$ и $\Phi_z = \{F_1, F_2, ..., F_k\}$. При значениях $wt(\{a_1, a_2, ..., a_k\}) = 1$ условие (2.12) фактически является условием сбалансированности самих компонентных булевых функций.

Для полноты изложения материала коротко опишем алгоритм [80] построения криптографических S-блоков подстановки длины $N = 2^5 = 32$ на основе известного множества булевых функций Ψ с учетом (2.12):

Алгоритм А2:

Шаг 1. Инициализируем переменные цикла $\kappa = 1$, $a = 1$.

Шаг 2. Если $a > |\Psi|$, то построение S-блоков подстановки на основе данного множества булевых функций невозможно, иначе выбираем a-тую булеву функцию из множества Ψ.

Шаг 3. Проверяем выполнение условия сбалансированности линейных комбинаций (2.12). Если она выполняется, то $\kappa = \kappa + 1$, $a = a + 1$ и переходим к Шагу 4, иначе $a = a + 1$ и возвращаемся на Шаг 2.

Шаг 4. Если $\kappa < 5$ возвращаемся на Шаг 2, иначе построение завершено.

Применяя данный алгоритм с разными начальными значениями a на Шаге 1 возможно построить $J = 4578$ оптимальных S-блоков подстановки длины $N = 32$, которые удовлетворяют критериям высокой нелинейности и нулевой корреляции векторов выхода и входа, один из которых

$$S_5 = \{28,24,4,18,2,25,1,14,22,5,11,10,23,29,17,15,9,3,13, \\ 21,6,19,31,30,26,7,27,20,12,8,16,0\}. \quad (2.13)$$

Данная подстановочная конструкция имеет корреляционный иммунитет порядка $m = 1$, и соответственно ее матрица коэффициентов корреляции

$$R = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \quad (2.14)$$

Также, для подстановочной конструкции (2.13) выполняется строгий лавинный критерий, соответственно матрица весов производных ее компонентных булевых функций имеет вид.

Таблица 2.6

Таблица весов производных компонентных булевых функций

e_u	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$
00001	16	16	16	16	16
00010	16	16	16	16	16
00100	16	16	16	16	16
01000	16	16	16	16	16
10000	16	16	16	16	16

Приведем также распределение расстояний нелинейности N_f и алгебраических степеней нелинейности [35] по компонентным булевым функциям S-блока подстановки (2.13)

F_j	F_1	F_2	F_3	F_4	F_5
N_F	8	8	8	8	8
$\deg(F)$	2	3	3	2	2

. (2.15)

Тем не менее, длина построенных криптографических S-блоков подстановки, которые удовлетворяют как строгому лавинному критерию, так и критерию нулевой корреляции векторов выхода и входа недостаточна для применения в современных криптографических алгоритмах, например Rijndael/AES [30], где $N = 2^8 = 256$.

Для увеличения длины построенных криптографических S-блоков подстановки целесообразно использовать **Алгоритм А1** [2], проиллюстрированный в параграфе 2.1.

Алгоритм А1 для приведенного случая может быть проиллюстрирован в виде схемы, изображенной на рис. 2.1, где x_j — входная последовательность бит S-блока подстановки, y_j — его исходная последовательность бит.

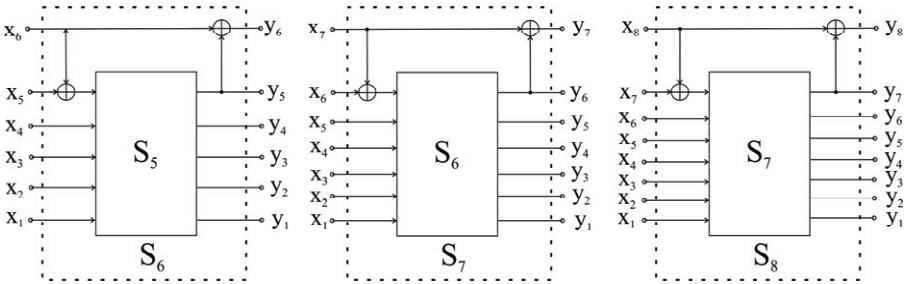


Рис. 2.3. Алгоритм А2 рекуррентного увеличения длины S-блока подстановки

Таким образом, имея криптографический S-блок подстановки длины $N = 2^5 = 32$ с помощью рекуррентного алгоритма увеличения длины можно получить криптографический S-блок подстановки длины $N = 2^8 = 256$. Причем, исследования позволили установить следующие свойства данного алгоритма:

Свойство 1. Алгоритм А1 не меняет исходный порядок m корреляционного иммунитета S-блока подстановки.

Свойство 2. Алгоритм А1 не меняет весов производных $wt\left(D_{j,u}\right),\ j,u = \overline{1,k}$ компонентных булевых функций F_j S-блока подстановки.

Свойство 3. Алгоритм А1 не меняет алгебраической степени нелинейности $\min\left\{\deg\left(F_j\right)\right\}$, $j = \overline{1,k}$ S-блока подстановки.

Свойство 4. На каждой итерации Алгоритм А1 удваивает расстояние нелинейности N_S S-блока подстановки.

Применяя данный Алгоритм А1 (рис. 2.3) к S-блоку подстановки (2.13) получаем новый криптографический S-блок подстановки (табл. 2.7) длины $N = 2^8 = 256$, который в соответствии со свойствами рекуррентного алгоритма сохраняет соответствие как строгому лавинному критерию, так критерию нулевой корреляции его выходных и входных векторов.

Таблица 2.7

Построенный S-блок подстановки большой длины

S_8	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	5C	58	04	F2	02	F9	A1	AE	F6	05	AB	AA	57	5D	F1	0F
1	A9	A3	0D	F5	06	F3	5F	5E	FA	07	5B	54	AC	A8	F0	00
2	B8	BC	12	E4	19	E2	4E	41	E5	16	4A	4B	BD	B7	EF	11
3	43	49	15	ED	13	E6	BE	BF	E7	1A	B4	BB	48	4C	E0	10
4	98	9C	32	C4	39	C2	6E	61	C5	36	6A	6B	9D	97	CF	31
5	63	69	35	CD	33	C6	9E	9F	C7	3A	94	9B	68	6C	C0	30
6	7C	78	24	D2	22	D9	81	8E	D6	25	8B	8A	77	7D	D1	2F
7	89	83	2D	D5	26	D3	7F	7E	DA	27	7B	74	8C	88	D0	20
8	D8	DC	72	84	79	82	2E	21	85	76	2A	2B	DD	D7	8F	71
9	23	29	75	8D	73	86	DE	DF	87	7A	D4	DB	28	2C	80	70
A	3C	38	64	92	62	99	C1	CE	96	65	CB	CA	37	3D	91	6F
B	C9	C3	6D	95	66	93	3F	3E	9A	67	3B	34	CC	C8	90	60
C	1C	18	44	B2	42	B9	E1	EE	B6	45	EB	EA	17	1D	B1	4F
D	E9	E3	4D	B5	46	B3	1F	1E	BA	47	1B	14	EC	E8	B0	40
E	F8	FC	52	A4	59	A2	0E	01	A5	56	0A	0B	FD	F7	AF	51
F	03	09	55	AD	53	A6	FE	FF	A7	5A	F4	FB	08	0C	A0	50

В соответствии со Свойствами 1—4 данный S-блок подстановки имеет идеальную матрицу коэффициентов корреляции $r_{v,\mu}$ (1.9) векторов выхода y_j и векторов входа x_j

$$R = \begin{bmatrix} 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0 \end{bmatrix}, \qquad (2.16)$$

а также отвечает строгому лавинному критерию (табл. 2.8).

Таблица 2.8

Веса производных компонентных булевых функций построенного S-блока подстановки

e_j	$wt(D_{1,k})$	$wt(D_{2,k})$	$wt(D_{3,k})$	$wt(D_{4,k})$	$wt(D_{5,k})$	$wt(D_{6,k})$	$wt(D_{7,k})$	$wt(D_{8,k})$
10000000	128	128	128	128	128	128	128	128
01000000	128	128	128	128	128	128	128	128
00100000	128	128	128	128	128	128	128	128
00010000	128	128	128	128	128	128	128	128
00001000	128	128	128	128	128	128	128	128
00000100	128	128	128	128	128	128	128	128
00000010	128	128	128	128	128	128	128	128
00000001	128	128	128	128	128	128	128	128

Причем расстояния и алгебраическая степень нелинейности у построенного S-блока подстановки выходит немного выше чем в [24] и [25].

F_j	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
N_F	64	64	64	64	64	64	64	64
$\deg(F)$	2	3	3	2	2	2	2	2

. (2.17)

Таким образом, можем записать метод синтеза S-блоков подстановки, которые отвечают, как строгому лавинному критерию, так и критерию нулевой корреляции выходных и входных векторов S-блока подстановки:

Шаг 1. Находим (даже переборным методом) множество булевых функций Ψ, которые отвечают как строгому лавинному критерию, так и критерию нулевой корреляции векторов выхода и входа S-блока подстановки.

Шаг 2. Используя Алгоритм А2 синтезируем на их основе множество S-блоков подстановки, удовлетворяющих как строгому лавинному критерию, так и критерию нулевой корреляции векторов выхода и входа S-блока подстановки длины $N = 32$.

Шаг 3. Используя Алгоритм А1 проводим рекуррентное увеличение длины построенных на предыдущем шаге S-блоков подстановки к $N = 256$, или больше.

Очевидно, применяя Алгоритм А1 можно построить $J = 4578$ искомых криптографических S-блоков подстановки полученных в результате применения Алгоритма А2. Каждый из них состоит из компонентных булевых функций F_j, $j = \overline{1,8}$, которые обладают корреляционным иммунитетом и удовлетворяют строгому лавинному критерию. Изменение порядка следования функций F_j, которое можно провести 8!=40320 способами, а также все возможные их знаковые кодирования, которых может быть $2^8 = 256$ комбинаций не приведут к потере S-блоком подстановки криптографического качества. Таким образом, мощность класса синтезированных оптимальных S-блоков подстановки будет определяется как

$$W = 4578 \cdot 40320 \cdot 256 = 4.7254 \cdot 10^{10} \approx 2^{35}, \qquad (2.18)$$

что в принципе является существенным с криптографической точки зрения.

ГЛАВА 3
МЕТОДЫ СИНТЕЗА ВЫСОКОНЕЛИНЕЙНЫХ S-БЛОКОВ ПОДСТАНОВКИ

3.1. Метод синтеза S-блоков подстановки конструкции Ниберг на основе полных классов неприводимых полиномов

Практически ценными являются S-блоки подстановки конструкции Ниберг, которые описываются выражениями (1.3), (1.4). S-блоки данной конструкции обладают многими привлекательными криптографическими качествами, такими как: равномерная минимизация коэффициентов корреляции, высокое расстояние нелинейности в смысле расстояния от компонентных булевых функций до аффинного кода, блочная структура, близкая к оптимальной.

Из анализа (1.3) и (1.4) можно сделать вывод, что качество S-блоков подстановки конструкции Ниберг зависит от выбора вида неприводимого полинома $f(z)$ степени k, из полного множества неприводимых полиномов W_k, а также от выбора вида матрицы аффинного преобразования A, из полного множества матриц аффинных преобразований W_A.

Основные результаты исследования зависимости криптографических свойств S-блоков подстановки от вида выбранного полинома приведены в [41].

Для построения биективного нелинейного преобразования согласно формуле (1.3) в качестве $f(z)$ возможно применение неприводимых, а также первообразных неприводимых полиномов [74]. Известно, что количество, неприводимых q-ичных полиномов заданной степени k определяется как

$$|W_k| = \frac{1}{k} \sum_{d \mid \mathrm{k}}^{d} \mu(d) \cdot q^{(k/d)} , \qquad (3.1)$$

где d — делители числа k ;

$\mu(d)$ — функция Мёбиуса [81];

запись $d \mid k$ означает, что d делит k нацело.

В этом множестве W_k существует множество первообразных полиномов мощности

$$|V_k| = \frac{\varphi\left(q^k - 1\right)}{k}, \tag{3.2}$$

где $\varphi(x)$ — фи-функция Эйлера.

Например, для преобразования Rijndael при длине S-блока подстановки $N = 256$ $|W_8| = 30$, $|V_8| = 16$. Согласно конструктивному алгоритму синтеза [82, 83] построим все неприводимые полиномы степени $k = 8$ и для краткости запишем их в виде соответствующих десятичных эквивалентов

$$\left(f_i(z)\right)_{10} = \left\{\begin{array}{l} 283,\ \mathbf{285},\ \mathbf{299},\ \mathbf{301},\ 313,\ 319,\ \mathbf{333},\ \mathbf{351},\ \mathbf{355},\ \mathbf{357},\ \mathbf{361},\ \mathbf{369},\ 375,\ 379, \\ \mathbf{391},\ 395,\ \mathbf{397},\ 415,\ 419,\ \mathbf{425},\ 433,\ 445,\ \mathbf{451},\ \mathbf{463},\ 471,\ 477,\ \mathbf{487},\ 499, \\ \mathbf{501},\ 505 \end{array}\right\}, \tag{3.3}$$

где первообразные неприводимые полиномы выделены жирным шрифтом своих десятичных эквивалентов. Изучение зависимости криптографических характеристик преобразования Rijndael от вида неприводимого полинома, который используется для построения S-блока подстановки, включило в себя параметры, приведенные в первой главе, а также специфические параметры, которые касаются блочной структуры компонентных булевых функций, а именно, распределение длин $|\beta|$ блоков β, входящих в состав компонентных булевых функций нелинейного преобразования. Для нелинейного преобразования на основе полинома Rijndael $f(z) = z^8 + z^4 + z^2 + z + 1$ приведем матрицу B распределения длин блоков для каждой компонентной булевой функции

$$B=\begin{Bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & |\beta| \\ 68 & 30 & 14 & 8 & 1 & 5 & 1 & 0 & 0 & 0 & 1 & F_1 \\ 51 & 29 & 17 & 7 & 7 & 4 & 0 & 0 & 0 & 0 & 0 & F_2 \\ 72 & 40 & 10 & 9 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & F_3 \\ 76 & 31 & 16 & 3 & 6 & 2 & 1 & 0 & 0 & 0 & 0 & F_4 \\ 55 & 28 & 13 & 14 & 4 & 0 & 3 & 0 & 0 & 0 & 0 & F_5 \\ 57 & 29 & 20 & 9 & 5 & 1 & 0 & 0 & 0 & 0 & 0 & F_6 \\ 65 & 40 & 12 & 7 & 5 & 1 & 1 & 0 & 0 & 0 & 0 & F_7 \\ 55 & 28 & 23 & 7 & 4 & 0 & 2 & 0 & 0 & 0 & 1 & F_8 \end{Bmatrix}, \qquad (3.4)$$

где первая строка матрицы B содержит все возможные длины $|\beta|$ блоков. Очевидно, что в этом случае величина $|\beta|_{\max}=11$. Приведем описание криптографических характеристик S-блока на базе полного класса неприводимых полиномов (3.3) степени $k=8$ согласно параметрам, которые оцениваются (табл. 3.1).

Таблица 3.1

Криптографические характеристики S-блоков на базе полного класса несводимых полиномов, $k=8$ $N=256$

i	$(f_i(z))_{10}$	$\max\{r_{i,j}\}$	K^0	N_s	$\mu_{\min}\ldots\mu_{\max}$	$\lvert\beta\rvert_{\max}$
1	285	0,125	4	112	118…132	15
2	299	0,1094	7	112	120…136	10
3	301	0,1094	3	112	114…134	14
4	333	0,1094	7	112	120…136	13
5	351	0,125	3	112	126…138	10
6	355	0,1094	1	112	126…134	9
7	357	0,0938	3	112	118…136	9
8	361	0,125	5	112	116…132	11
9	369	0,1094	5	112	120…134	9
10	391	0,1094	5	112	112…136	11
11	397	0,1094	4	112	122…140	10
12	425	0,1094	10	112	118…142	9
13	451	0,1094	7	112	124…138	14
14	463	0,125	3	112	122…142	9
15	487	0,125	8	112	118…142	10
16	501	0,0938	4	112	124…134	13
17	283	0,125	4	112	116…138	11
18	313	0,0938	10	112	118…132	16
19	319	0,125	7	112	118…136	11
20	375	0,1094	3	112	124…138	11
21	379	0,125	2	112	116…142	10

Окончание табл. 3.1

22	395	0,125	9	112	122…140	10
23	415	0,125	8	112	120…140	9
24	419	0,1094	2	112	124…138	12
25	433	0,125	6	112	118…142	10
26	445	0,1094	5	112	120…136	10
27	471	0,1094	4	112	114…138	10
28	477	0,125	2	112	116…128	10
29	499	0,0938	1	112	122…138	9
30	505	0,125	5	112	126…142	9

Полученные данные свидетельствуют о разнообразии выбора полиномов для использования в блочных шифрах согласно решению выбора, того или иного критерия криптографического качества. Например, если выбран критерий равномерной минимизации матрицы коэффициентов корреляции, то целесообразнее всего использовать полиномы для нахождения обратных элементов с минимальным количеством нулей K^0, например, $f_6 = (355)_{10}$, $f_{29} = (499)_{10}$. Применение данных полиномов позволит затруднить линейную аппроксимацию шифра аффинными булевыми функциями [84], увеличивая его резистивность атакам линейного криптоанализа. Эти полиномы имеют лучшие (минимальные) значения корреляции векторов выхода и входа S-блока, в сравнении с полиномом, применяемым в алгоритме Rijndael/AES.

Если выбран критерий отсутствия корреляции векторов выхода и входа, то лучшими будут полиномы $f_{12} = (425)_{10}$, $f_{18} = (313)_{10}$. Они имеют наибольшее количество нулей K^0 в матрицах коэффициентов корреляции векторов выхода и входа, что затруднит корреляционный криптоанализ, однако упростит аппроксимацию шифра аффинными булевыми функциями за счет большего количества единичных значений элементов в полной матрице коэффициентов корреляции со всеми аффинными функциями.

Отметим, что компонентные булевы функции F_i, $i = \overline{1,8}$, имеют количество блоков μ, близкое к оптимальному значению, равному $\mu_0 = N/2$ [85], а также не содержат в своем составе слишком длинных

последовательностей одинаковых символов. Это позволяет говорить о высоком качестве автокорреляционных свойств компонентных булевых функций в смысле малых значений их боковых лепестков.

Более высокая алгебраическая степень нелинейности $\deg(F_i)$ компонентных булевых функций позволяет эффективно противостоять атакам линейного криптоанализа, затрудняя аппроксимацию шифра системами линейных уравнений. Критерий высокой алгебраической степени нелинейности можно модифицировать, потребовав, чтобы алгебраическая степень нелинейности была константой для множества ψ всех циклических сдвигов $\tau = \overline{0,255}$ компонентных булевых функций

$$\psi = \left\{ D^{\tau} F_i \right\}, \quad \tau = \overline{0, 2^k - 1}, \quad i = \overline{1,8}, \tag{3.5}$$

где D — оператор циклического сдвига.

Проведенные исследования позволили получить распределение алгебраических степеней нелинейности для компонентных булевых функций нелинейного преобразования шифра Rijndael

$$Z = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \deg(F_i) \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 & F_1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 8 & 248 & 0 & F_2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 12 & 244 & 0 & F_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 & F_4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 & F_5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 & F_6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 & F_7 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 256 & 0 & F_8 \end{bmatrix}, \tag{3.6}$$

где первая строка матрицы Z определяет все возможные численные значения величины $\deg(F_i)$.

Таким образом, для нелинейного преобразования на основе обратных элементов по модулю неприводимого полинома Rijndael лишь для компонентных булевых функций F_2 и F_3 существуют такие значения

циклических сдвигов τ, для которых алгебраические степени нелинейности отличаются от алгебраической степени нелинейности при $\tau = 0$.

Установлено, что существует множество таких неприводимых полиномов, для которых при любом значении циклического сдвига τ, алгебраическая степень нелинейности всех компонентных булевых функций нелинейного преобразования остается постоянной $\deg(f) = 7$. Исследования позволили найти множество Ω всех таких полиномов в множестве неприводимых полиномов степени $k = 8$

$$\Omega = \{285,351,355,463,313,319,375,379,395,415,419,433,471,477,505\}. \quad (3.7)$$

Полиномы множества Ω обеспечивают свойство инвариантности алгебраической степени нелинейности компонентных булевых функций относительно циклического сдвига $\tau = \overline{0,255}$.

Конструктивным недостатком нелинейного преобразования конструкции Ниберг на основе обратных элементов (1.3) являются малые периоды возврата S-блока в исходное состояние $T = 2$ [59]. Возможность устранения данного недостатка лежит в использовании полной конструкции Ниберг (1.3), (1.4), которая включает аффинное преобразование вида $y = A \cdot x + b$, позволяющее существенно увеличить периоды возврата S-блока в исходное состояние T. Количество всех существующих аффинных преобразований определяется соотношением [86]

$$\left|W_A\right|_k = \prod_{i=0}^{k-1}\left(2^k - 2^i\right). \quad (3.8)$$

Например, для $k = 8$ находим $\left|W_A\right|_8 \approx 5{,}3 \cdot 10^{18}$. В криптографическом алгоритме Rijndael используется одно из таких аффинных преобразований вида [30]

$$A_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad a = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, \tag{3.9}$$

которое позволяет увеличить период возврата S-блока в исходное состояние до величины $T_1 = 1\,531\,530$. Аффинное преобразование, которое увеличивает период возврата S-блока в исходное состояние T нелинейного элемента, может быть подобрано индивидуально для каждого полинома так, чтобы максимизировать данную величину. Например, матрица преобразования

$$A_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad a = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tag{3.10}$$

позволяет получить период возврата S-блока подстановки в исходное состояние $T_2 = 14\,408\,856$ при работе с нелинейным элементом на основе полинома Rijndael.

3.2. Метод синтеза S-блоков на основе критерия максимального лавинного эффекта

В последнее время усиленное внимание уделяется вопросам синтеза нелинейных модифицированных S-блоков конструкции Ниберг [16], удовлетворяющих критерию максимального лавинного эффекта [87], применительно к шифру Rijndael/AES [30].

Основные результаты по указанному направлению можно найти в [88].

Для полноты изложения материала статьи приведем сущность метода построения S-блоков, удовлетворяющих критерию максимального лавинного эффекта [87]. Пусть $X=[x_i]$, $i=\overline{0,255}$, — последовательность возрастающих чисел от 0 до 255.

Исходную последовательность $Q=[q_i]$, $i=\overline{0,255}$ S-блока подстановки конструкции Ниберг представим с помощью таблицы истинности в виде её компонентных булевых функций

$$Q=[F_1;F_2;F_3;F_4;F_5;F_6;F_7;F_8], \tag{3.11}$$

где знак ";" означает вертикальную конкатенацию компонентных булевых функций длины $N=256$ каждая. Найдем производные $D_{i,k}=F_i(x)\oplus F_i(x\oplus e_k)$ каждой булевой функции по каждому направлению e_k веса $wt(e_k)=1$, где e_k — вектор с единицей на k-й позиции и нулями на остальных; $\oplus$ — операция суммирования по модулю 2. Построим таблицу (табл. 3.2) весов производных компонентных булевых функций $wt\left(D_{i,k}\right)$.

Таблица 3.2

Таблица весов производных компонентных булевых функций

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	136	124	128	116	120	140	124	124
01000000	124	124	120	120	140	124	124	136
00100000	124	136	132	140	124	132	136	124
00010000	136	144	120	124	132	128	124	124
00001000	144	124	128	132	128	120	124	136
00000100	124	140	132	128	120	132	136	144
00000010	140	124	136	120	132	120	144	124
00000001	124	132	124	132	120	128	124	140

Определение [87]. Нелинейный S-блок обладает критерием максимального лавинного эффекта если все веса $wt\left(D_{i,k}\right)$ всех производных его

компонентных булевых функций по всем направлениям единичного веса имеют значения, равные не меньше половины длины S-блока

$$wt\left(D_{i,k}\right) \geq N/2 = 128,\ i,k = \overline{1,8}. \tag{3.12}$$

Из анализа данных конструкции (табл.3.2) приходим к выводу о том, что S-блок конструкции Ниберг, применяемы в Rijndael/AES не обладает свойством максимального лавинного эффекта. Поэтому в работе [87] предложен следующий метод **M1** построения S-блоков, удовлетворяющих критерию максимального лавинного эффекта.

Шаг 1. Выберем произвольно невырожденную матрицу аффинного преобразования A, например

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{3.13}$$

Зафиксируем первые 7 её строк, а восьмибитное двоичное число, представляемое восьмой строкой, принимает значения от 0 до 255 т.е. все $2^8 = 256$ возможных значений. Найдем все такие структуры восьмой строки, при которых вес производной $wt\left(D_{8,k}\right) \geq 128$. Найденные 10 структур восьмой строки поместим в множество Ψ, в шестнадцатеричной системе счисления

$$\Psi = \{0\text{D},\ 1\text{B},\ 24,\ 37,\ 52,\ 6\text{F},\ 86,\ 92,\ \text{A9},\ \text{DF}\}_h\ . \tag{3.14}$$

Установлено, что построение такой матрицы аффинного преобразования A, которая бы позволяла S-блоку конструкции Ниберг соответствовать критерию максимального лавинного эффекта возможно тогда, и только тогда, когда объем $|\Psi| \geq k$, что является необходимым условием.

Шаг 2. На основании данных множества (3.14) построим $C_{10}^{8}=45$ квадратных матриц размера (8×8), из которых отберем 20 уникальных конструкций аффинного преобразования, позволяющих получить 20 уникальных S-блоков, удовлетворяющих критерию максимального лавинного эффекта. Например, рассмотрим одну из матриц $A=\left[1\text{B},\ 37,\ 52,\ 6\text{F},\ 86,\ 92,\ \text{A9},\ \text{DF}\right]^{T}$, которая в двоичном виде представляется как

$$A=\begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}. \tag{3.15}$$

Применив данное преобразование (3.15) к S-блоку конструкции Ниберг получаем новый S-блок, удовлетворяющий критерию максимального лавинного эффекта, как это видно из анализа табл. 3.3

Таблица 3.3

Таблица весов производных компонентных булевых функций

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	144	132	140	128	140	128	132	132
01000000	132	128	144	132	136	132	140	136
00100000	128	132	128	136	144	128	144	132
00010000	132	136	136	132	132	136	128	136
00001000	136	132	136	136	128	132	136	132
00000100	132	136	128	132	132	144	136	128
00000010	136	132	136	128	136	136	128	128
00000001	132	128	136	128	132	128	136	136

Шаг 3. Варьируя значения вектора сдвига b добиваемся наилучших корреляционных свойств S-блока. Экспериментально установлено, что структура вектора сдвига b не оказывает влияния на вид матрицы расстояний производных компонентных булевых функций. Очевидны модификации

рассмотренного метода поиска подходящих аффинных преобразований для каждого неприводимого полинома $f(z)$.

Анализ данного метода также органично ставит задачу поиска таких неприводимых полиномов, для которых существует подходящая матрица аффинного преобразования A, при котором S-блок удовлетворяет критерию максимального лавинного эффекта.

В криптоалгоритме Rijndael/AES при значениях $q=2$, $k=8$ количество неприводимых полиномов, в соответствии с формулой (3.1) достигает $\left|f_2^8\right|=30$, что является криптографически незначительной величиной. Однако, в работе [89] предложен метод построения полного класса неприводимых полиномов над всеми изоморфными представлениями поля $GF(q)$. Например, рассмотрим поле $GF(256)$, которое имеет следующие свои изоморфные представления

$$GF(256) => GF(2^8) => GF(4^4) => GF(16^2), \tag{3.16}$$

среди которых в соответствии с выражением (3.1) в поле $GF(2^8)$ имеется $\left|f_2^8\right|=30$ неприводимых полиномов, в поле $GF(4^4)$ имеется $\left|f_4^4\right|=60$ неприводимых полиномов, а в поле $GF(16^2)$ имеется $\left|f_{16}^2\right|=720$ неприводимых полиномов. Таким образом, количество неприводимых полиномов над всеми изоморфными представлениями поля $GF(256)$ определяется как

$$J=\left|f_2^8\right|+1\cdot\left|f_4^4\right|+\left|f_{16}^2\right|=30+60+720=810. \tag{3.17}$$

Проведенный экспериментальный анализ всех 810-ти криптографических S-блоков, построенных на базе всех неприводимых полиномов (10) показал, что для них характерны криптографически привлекательные свойства, а именно: равномерная минимизация матрицы коэффициентов корреляции, высокое расстояние нелинейности $N_s=112$, высокая алгебраическая степень нелинейности $\deg(F_i)=7$, $i=\overline{1,8}$.

Сведем в табл. 3.4 данные о количестве подходящих пар $\{f(z), A\}$, которые обеспечивают построение оптимальных S-блоков по критерию максимального лавинного эффекта.

Таблица 3.4

Данные о количестве подходящих пар $\{f(z), A\}$

Изоморфное представление поля $GF(256)$	Неприводимый полином	$\lvert\Psi\rvert$	Количество подходящих матриц
$GF\left(2^8\right)$	$f(z)=z^8+z^6+z^3+z^2+1$	10	20
	$f(z)=z^8+z^6+z^5+z^2+1$	10	20
	$f(z)=z^8+z^6+z^5+z^4+z^3+z+1$	9	5
	$f(z)=z^8+z^7+z^5+z^4+z^3+z^2+1$	9	5
$GF\left(4^4\right)$	$f(z)=z^4+z^2+2z+3$	14	1073
	$f(z)=z^4+z^2+3z+2$	14	1073
	$f(z)=z^4+2z^2+2z+2$	14	723
	$f(z)=z^4+2z^2+3z+1$	16	5519
	$f(z)=z^4+3z^2+2z+1$	16	5519
	$f(z)=z^4+3z^2+3z+3$	14	723
	$f(z)=z^4+z^3+z^2+2$	14	723
	$f(z)=z^4+z^3+z^2+3$	14	723
	$f(z)=z^4+z^3+2z^2+z+1$	11	89
	$f(z)=z^4+z^3+3z^2+z+1$	11	89
	$f(z)=z^4+2z^3+3z^2+1$	16	5519
	$f(z)=z^4+2z^3+3z^2+3$	14	1073
	$f(z)=z^4+3z^3+2z^2+1$	16	5519
	$f(z)=z^4+3z^3+2z^2+2$	14	1073

Анализируя результаты табл. 3.4 нетрудно установить, что общее количество существующих над изоморфными представлениями поля $GF(256)$ S-блоков конструкции Ниберг, которые удовлетворяют критерию максимального лавинного эффекта, определяется величиной $V_1 = 29\,488$, из которых $V_2 = 50$ были построены в [87].

Найдено также, что неприводимые полиномы над изоморфным представлением поля $GF\left(16^2\right)$ не позволяют строить S-блоки по критерию максимального лавинного эффекта.

Рассмотрим пример построения S-блока конструкции Ниберг над изоморфным представлениям поля $GF(4^4)$, соответствующего критерию максимального лавинного эффекта. Пусть задан полином $f(z) = z^4 + 3z^3 + 2z^2 + 2$, тогда можем построить S-блок конструкции Ниберг, таблица замены которого представляется в виде табл. 3.5 с шестнадцатеричным представлением элементов (без аффинного преобразования).

Таблица 3.5

S-блок конструкции Ниберг

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	03	02	E4	D0	F0	49	9C	C7	B0	A0	78	50	8E	60
1	39	5A	55	CB	34	B9	D7	75	3C	68	64	77	F6	C9	30	AB
2	27	86	F5	FF	AD	56	87	20	2C	EF	67	BE	28	EE	D4	DC
3	1E	AA	4D	AF	14	B8	99	BC	5B	10	FD	4E	18	69	9A	DE
4	EA	47	E2	B4	6E	70	EB	41	F1	07	B2	7B	AE	32	3B	FC
5	0D	79	C4	D2	CA	12	25	AC	A9	84	11	38	F9	5F	F8	5D
6	0F	8F	9F	F2	1A	76	BF	2A	19	3D	BB	EC	81	94	44	71
7	45	6F	7E	C1	D6	17	65	1B	0C	51	B3	4B	B6	CD	72	C0
8	95	6C	CE	91	59	A8	21	26	D9	C3	E0	96	A3	E6	0E	61
9	CF	83	DA	E9	6D	80	8B	E1	BD	36	3E	DF	08	C6	F3	62
A	0B	B1	E7	8C	A7	FB	FA	A4	85	58	31	1F	57	24	4C	33
B	0A	A1	4A	7A	43	E3	7C	CC	35	15	ED	6A	37	98	2B	66
C	7F	73	D8	89	52	D3	9D	09	F7	1D	54	13	B7	7D	82	90
D	05	E5	53	C5	2E	DD	74	16	C2	88	92	E8	2F	D5	3F	9B
E	8A	97	42	B5	04	D1	8D	A2	DB	93	40	46	6B	BA	2D	29
F	06	48	63	9E	FE	22	1C	C8	5E	5C	A6	A5	4F	3A	F4	23

при этом таблица (табл. 3.6) весов производных компонентных булевых функций — $wt\left(D_{i,k}\right)$ имеет вид

Таблица 3.6

Таблица весов производных компонентных булевых функций

e_k	$wt\left(D_{1,k}\right)$	$wt\left(D_{2,k}\right)$	$wt\left(D_{3,k}\right)$	$wt\left(D_{4,k}\right)$	$wt\left(D_{5,k}\right)$	$wt\left(D_{6,k}\right)$	$wt\left(D_{7,k}\right)$	$wt\left(D_{8,k}\right)$
10000000	132	128	132	124	124	128	128	124
01000000	136	132	128	132	132	124	132	128
00100000	132	124	124	120	120	120	136	132
00010000	128	132	120	124	124	120	128	136
00001000	124	120	128	132	120	140	128	132
00000100	120	124	136	128	136	120	124	128
00000010	128	132	132	144	116	132	120	124
00000001	136	128	136	132	132	116	120	120

Как видно из анализа конструкции (табл. 3.6), не все компонентные булевы функции S-блока достигают максимального лавинного эффекта. В соответствии с описанным методом, находим множество Ψ для заданного вида S-блока (табл. 3.5)

$$\Psi = \{17,2B,3A,5F,66,69,AD,B5,B6,BE,D7,D9,ED,FB,\}_h . \qquad (3.18)$$

Поскольку выполняется неравенство $|\Psi| \geq 8$ — необходимое условие построения матрицы аффинного преобразования A, позволяющей достижение S-блоком критерия максимального лавинного эффекта выполняется.

Построим матрицу аффинного преобразования A. В нашем примере было установлено, что всего на основе множества Ψ из (3.18) может быть построено $|A_i| = 1073$ таких матриц и соответственно новых S-блоков удовлетворяющих критерию максимального лавинного эффекта. Например, рассмотрим одну из матриц $A = [66,B5,B6,BE,D7,D9,ED,FB]^T$. Применив данное преобразование к S-блоку (табл. 3.5) получим новый S-блок (табл. 3.7)

Таблица 3.7

S-блок, соответствующий критерию максимального лавинного эффекта

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	F2	6F	9D	9F	B1	7E	EB	F7	3F	8F	31	68	4F	D4	3E
1	6B	3A	E2	88	2E	95	81	2D	C6	D6	61	B0	BC	15	71	B6
2	FF	3C	D3	A6	74	8D	CE	CF	78	18	0E	A5	27	EA	EE	06
3	94	44	B4	E9	E1	67	5A	38	C8	BE	3B	DB	56	24	35	9B
4	B5	C1	5D	D0	14	80	47	03	8C	30	12	07	1B	EC	F6	C9
5	45	9A	50	2C	7A	23	62	86	2B	A1	4C	99	64	97	96	0A
6	D8	26	98	E3	CB	42	57	BA	A4	34	08	77	0C	1F	AE	72
7	5C	E6	AA	FD	73	8E	93	39	B7	BD	E0	76	4D	4A	1D	0F
8	ED	89	25	B2	55	D9	3D	0D	AB	60	C0	82	5E	02	2A	CC
9	D7	91	C4	DA	7B	FE	79	32	CA	B3	5B	69	E8	CD	11	A3
A	87	7D	F0	49	01	F9	0B	6E	53	A7	83	66	7F	90	46	1E
B	75	C3	84	F5	9E	AF	37	B8	DC	13	85	4B	41	A8	48	FC
C	58	EF	59	E4	D2	DE	05	1A	4E	FB	10	D1	BF	C5	63	40
D	AD	6D	20	A2	E5	F4	DF	7C	92	16	DD	28	17	1C	A9	C7
E	8B	70	6C	22	5F	43	BB	AC	36	2F	F1	33	B9	FA	8A	D5
F	C2	19	51	6A	54	52	09	E7	65	F8	F3	9C	29	04	21	A0

Приведенный S-блок всецело соответствует критерию максимального лавинного эффекта, что подтверждается его таблицей (табл. 3.8) весов производных компонентных булевых функций

Таблица 3.8

Таблица весов производных компонентных булевых функций

e_k	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$	$wt(D_{1,k})$
10000000	132	132	136	128	136	132	136	144
01000000	136	132	132	132	128	132	132	132
00100000	136	144	132	144	136	132	136	136
00010000	144	136	132	132	144	136	132	132
00001000	136	132	132	136	128	136	132	136
00000100	128	128	136	132	136	144	132	132
00000010	128	132	136	136	128	136	132	132
00000001	132	128	144	132	136	128	136	132

Таким образом, можем описать предлагаемый метод построения S-блоков конструкции Ниберг с максимальным лавинным эффектом над всеми изоморфными представлениями поля $GF(256)$ в виде конкретных шагов:

Шаг 1. В соответствии с предварительно рассчитанными данными (табл. 3) выбираем вид неприводимого полинома $f(z)$. Критерием выбора конкретного вида неприводимого полинома может быть количество подходящих матриц аффинного преобразования, приводящих к максимальному лавинному эффекту.

Шаг 2. Для выбранного на Шаге 1 неприводимого полинома осуществляем построение S-блока подстановки конструкции Ниберг.

Шаг 3. В соответствии с методом **M1** осуществляем синтез подходящих матриц аффинного преобразования.

Нетрудно видеть, что изменение порядка следования компонентных булевых функций из числа $8! = 40320$ сохраняет соответствие S-блока критерию максимального лавинного эффекта.

Каждый S-блок также может быть модифицирован $2^k = 256$ способами за счет выбора вектора сдвига b, который не влияет на матрицу весов $wt(D_{i,k})$. Таким образом, общее число построенных S-блоков по критерию

максимального лавинного эффекта определяется величиной $W = 29\,488 \cdot 8! \cdot 2^8 = 29\,488 \cdot 40320 \cdot 256 \approx 3 \cdot 10^{11}$, что является весьма привлекательным с криптографической точки зрения.

3.3. Метод синтеза S-блоков подстановки на основе композиционных кодов степенных вычетов

Существование большого количества разных алгебраических конструкций в расширенных полях Галуа делает их исследование привлекательным не только для поиска в них сигнальных конструкций с хорошими корреляционными свойствами [53], но и для синтеза больших семейств S-блоков подстановки, которые обладают высоким уровнем криптографического качества.

Основные результаты проведенных исследований приведены в работе [90].

Исследования показывают, что количество S-блоков подстановки, которые обладают столь же хорошими криптографическими качествами как и конструкция Ниберг может быть существенно увеличено за счет применения кодов r-ичных вычетов [53] вида

$$Q = \alpha^r \bmod d(f(z), p), \tag{3.19}$$

где α — каждый элемент поля Галуа.

На основе кодов r-ичных вычетов могут быть построены классы S-блоков подстановки существенной мощности, которые не уступают по криптографическому качеству конструкции Ниберг [41]. Для получения биективного S-блока подстановки с помощью кодов r-ичных вычетов нужно использовать такие значения степеней вычетов r, чтобы

$$НОД(r, 2^k - 1) = 1, \tag{3.20}$$

где k — степень расширения поля. Например, для $k = 8$, существует 128 таких чисел, для которых выполняется соотношения (3.20)

$$\mathrm{H}=\left[\begin{array}{c}1,\,2,\,4,\,7,\,8,\,11,\,13,\,14,\,16,\,19,\,22,\,23,\,26,\,28,\,29,\,31,\,32,\\ 37,\,38,\,41,\,43,\,44,\,46,\,47,\,49,\,52,\,53,\,56,\,58,\,59,\,61,\,62,\,64,\\ 67,\,71,\,73,\,74,\,76,\,77,\,79,\,82,\,83,\,86,\,88,\,89,\,91,\,92,\,94,\,97,\\ 98,\,101,\,103,\,104,\,106,\,107,\,109,\,112,\,113,\,116,\,118,\,121,\\ 122,\,124,\,127128,\,131,\,133,\,134,\,137,\,139,\,142,\,143,\,146,\\ 148,\,149,\,151,\,152,\,154,\,157,\,158,\,161,\,163,\,164,\,166,\,167,\\ 169,\,172,\,173,\,176,\,178,\,179,\,181,\,182,\,184,\,188,\;191,\,193,\\ 194,\,196,\,197,\,199,\,202,\,203,\,206,\,208,\,209,\,211,\,212,\,214,\\ 217,\,218\quad 223,\,224,\,226,\,227,\,229,\,232,\,233,\,236,\,239,\,241,\\ 242,\,244,\,247,\,248,\,251,\,253\quad 254\end{array}\right]. \qquad (3.21)$$

Исследования показывают, что только при некоторых значениях степеней вычетов r из множества H могут быть построены биективные S-блоки подстановки, которые удовлетворяют базовым критериям высокого криптографического качества. Причем, криптографические характеристики практически полностью зависят от степени вычетов r. Приведем множество Ω таких степеней r, для которых криптографическое качество S-блоков подстановки является наилучшим

$$\Omega=\{127,\,191,\,223,\,239,\,247,\,251,\,253,\,254\}. \qquad (3.22)$$

Следует отметить, что все числа данного множества являются членами последовательности A023689 [91] над полем $GF(2^8)$, предложенной Оливером Герардом, каждый элемент которой содержит точно 7 единиц в своем двоичном представлении.

Приведем табл. 3.9, содержащую значения основных показателей криптографического качества, а также характеристики блочной структуры компонентных булевых функций S-блоков подстановки на основе r-ичных вычетов, где $r\in\Omega$, для полинома $\left(f(z)\right)_{10}=283$, применяемого в шифре Rijndael/AES [30]. Анализ данных (табл. 3.9) позволяет сделать выводы о высоком криптографическом качестве S-блоков подстановки на основе кодов r-ичных вычетов.

Таблица 3.9

Криптографические характеристики S- блоков подстановки на основе степеней $r \in \Omega$ и полинома $\left(f(z)\right)_{10} = 283$

Десятичный эквивалент полинома, $\left(f(z)\right)_{10}$	r	$\max\left\{r_{i,j}\right\}$	K^0	N_s	$\mu_{\min} - \mu_{\max}$	$\lvert\beta\rvert_{\max}$	$\min\left\{\deg\left(F_i\right)\right\}$	T
283	127	0.10938	4	112	144 - 116	14	7	8
283	191	0.12500	4	112	132 - 126	9	7	4
283	223	0.10938	4	112	138 - 120	9	7	8
283	239	0.12500	4	112	134 - 116	9	7	2
283	247	0.10938	4	112	134 - 116	10	7	8
283	251	0.12500	4	112	140 - 116	11	7	4
283	253	0.10938	4	112	144 - 120	13	7	8
283	254	0.12500	4	112	138 - 116	11	7	2

Отметим, что построение полученных S-блоков подстановки, при сохранении их дистанционных свойств с аффинным кодом, а также алгебраической степени нелинейности может осуществляться по формуле

$$Q = (\omega\alpha^r + \nu) \bmod \mathrm{d}\left(\mathrm{f(z)}, \mathrm{p}\right), \tag{3.23}$$

где $\omega = \overline{1, q^k - 1}$, $\nu = \overline{0, q^k - 1}$ для каждого $r \in \Omega$. Таким образом, мощность полученного класса S-блоков подстановки составляет

$$J = q^k \cdot \left(q^k - 1\right) \cdot \left|V_k\right|, \tag{3.24}$$

что уже при степени неприводимого полинома $k = 8$, позволяет построить $J = 1\,044\,480$ S-блоков подстановки, которые обладают уровнем криптографического качества не хуже конструкции Ниберг.

Отметим, что в большинстве случаев при значениях $\omega > 1$ и $\nu > 0$ увеличивается период возврата S-блока подстановки в исходное состояние, а также меняется его матрица коэффициентов корреляции и блочная структура.

Проведенные исследования позволили установить, что S-блоки на основе кодов степенных вычетов обобщают конструкцию Ниберг, повторяя её при значении степени $r = 254$, что может быть использовано для замены операции обращения элементов операцией возведения в степень.

ГЛАВА 4
МЕТОДЫ СИНТЕЗА ЭКОНОМИЧНЫХ S-БЛОКОВ ПОДСТАНОВКИ НА ОСНОВЕ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕ БРЕЙНА

4.1 Определение последовательности де Брейна и построение S-блоков на её основе

Двоичная псевдослучайная Mg-последовательность периода $N = 2^k$, со свойством k-граммного распределения — последовательность, в которой каждая серия из k бит встречается на замкнутом цикле точно один раз [93].

Вопросы синтеза полных классов сигналов, которые владеют такими практически привлекательными для задач криптографии свойствами являются чрезвычайно актуальными.

В данной главе приведены эффективные методы построения Mg-последовательностей, как двоичных так и четверичных. Каждая построенная Mg-последовательность позволяет синтез высококачественного S-блока подстановки, криптографические показатели качества которого не уступают наилучшим S-блокам подстановки, а также допускают экономию ячеек памяти в k раз для их хранения, причем, четверичные Mg-последовательности, в отличии от двоичных, хотя и не позволяют экономить столь большое количество ячеек памяти, но позволяют существенным образом расширить объемы доступных S-блоков подстановки и тем самым улучшить их криптографическую стойкость.

Линейную Mg-последовательность можно построить на базе m-последовательности, которая порождается регистром сдвига с линейной обратной связью [93, 94], построенным согласно генераторному полиному $\rho(v)$,

степени $k = \deg\{\rho(v)\}$, путем добавления нуля к серии бит из $(k-1)$ нулей. Например, при $\rho(v) = v^4 + v + 1$, $k = 4$, Mg-последовательность и соответствующая ей десятичная Q-последовательность имеют вид:

$$\begin{array}{rl} Mg = & [1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0 \quad 1 \quad 0 \quad 0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 0]; \\ Q = & [15 \quad 14 \quad 12 \quad 8 \quad 0 \quad 1 \quad 2 \quad 4 \quad 9 \quad 3 \quad 6 \quad 13 \quad 10 \quad 5 \quad 11 \quad 7]. \end{array} \qquad (4.1)$$

Из анализа системы соответствия (4.1) вытекает, что каждая Mg-последовательность полностью определяет структуру и криптографические свойства S-блока подстановки, где $X = \{x_0, x_1, x_2, x_3\}$, $Y = \{y_0, y_1, y_2, y_3\}$ — векторы элементов, которые поступают на вход и снимаются с выходных линий S-блока соответственно.

При этом для хранения Mg-последовательности необходим в k раз меньший объем памяти, чем для хранения десятичной Q-последовательности, что представляет принципиально новое решение задачи построения компактных S-блоков подстановки, которое особенно перспективно для криптоалгоритмов, допускающих свободный выбор S-блоков подстановки, например, стандарта ГОСТ 28147-89 [33].

Таким образом, задача конструирования экономичных S-блоков подстановки становится тесно связанной с задачей синтеза таких совершенных алгебраических конструкций как последовательности де Брейна.

В настоящий момент существуют следующие методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения на основе:

— двойного сцепления кортежей векторов (Метод 1);

— учета структурных свойств Mg-последовательностей (Метод 2);

— целочисленных функций (Метод 3).

Основные результаты по методам синтеза Mg-последовательностей и экономичных S-блоков подстановки на их основе представлены в работе [22].

4.2 Метод синтеза на основе двойного сцепления кортежей

Пусть $V_k = \{A_i\}$, $i = \overline{0, 2^k - 1}$, линейное векторное пространство двоичных векторов размера k. Введем операции сцепления каждого вектора $A_i = [\alpha_{i,k-1}, \alpha_{i,k-2}, \cdots, \alpha_{i,0}]$, где младший разряд справа.

Определение 4.1. Операции сцепления $S0$ и $S1$ произвольного вектора $A_i \in V_k$ — сдвиг вектору A_i влево на один элемент со следующей конкатенацией, соответственно, символа 0 или символа 1 и получение двоичного вектора размера k, как это показано с помощью выражений

$$\begin{array}{ll} \text{Сцепление } S0 & \text{Сцепление } S1 \\ [\alpha_{i,k-2}, \cdots, \alpha_{i,0}, 0]; & [\alpha_{i,k-2}, \cdots, \alpha_{i,0}, 1] \end{array}. \qquad (4.2)$$

Определение 4.2. Период ε_1 сцепления вектора A_i по горизонтали — это минимальное число последовательных операций сцепления $S0$, при которых вектор A_i переходит в нулевой, то есть $A_i \to \bar{0}$.

Определение 4.3. Период ε_2 сцепления вектора A_i по вертикали это минимальное число последовательных операций сцепления $S1$, при которых вектор A_i переходит в единичный, то есть $A_i \to \bar{1}$.

На основе принятых определений установлены свойства операторов $S0$ и $S1$:

Свойство 4.1. Все четные векторы A_γ, $\gamma = 2i$ имеют максимальный период сцепления по вертикали $\varepsilon_2 = k + 1$ и так, образовывают вертикальный кортеж $C = \left[A_\gamma^{S0_{\varepsilon_2}}, A_\gamma^{S0_{\varepsilon_2 - 1}}, ..., A_\gamma^{S0_1} \right]^T$, где $A_\gamma^{S0_\iota}$ — ι последовательных операций сцепления $S0$ вектора A_γ, T — оператор транспонирования. Каждый вектор полученного кортежа C с помощью оператора $S0$ образовывает свой горизонтальный кортеж $D_u = \left[C_u^{S1_1}, ..., C_u^{S1_{\varepsilon_1 - 1}}, C_u^{S1_{\varepsilon_1}} \right]$, где $C_u^{S1_\iota}$ — ι последовательных операций сцепления $S1$

вектора C_u, $u = \overline{1,\varepsilon_2}$. Пусть множество всех построенных таким образом кортежей C и D_u образует хранилище кортежей вектора A_i. Пары четных векторов $\{A_\gamma, A_{\gamma+2^{k-1}}\}, i = \overline{0,2^{k-2}-1}$, назовем образующими. Ясно, что число таких пар

$$p = 2^{k-2}, k = 3,4,5,\cdots, \tag{4.3}$$

определяет число хранилищ для данного значения размерности k.

Свойство 4.2. Каждый образующий вектор из данной образующей пары формирует на основе операций сцепления $S0$ и $S1$ тождественно равные множества кортежей C и D_u, то есть тождественно равные хранилища кортежей, соответственно.

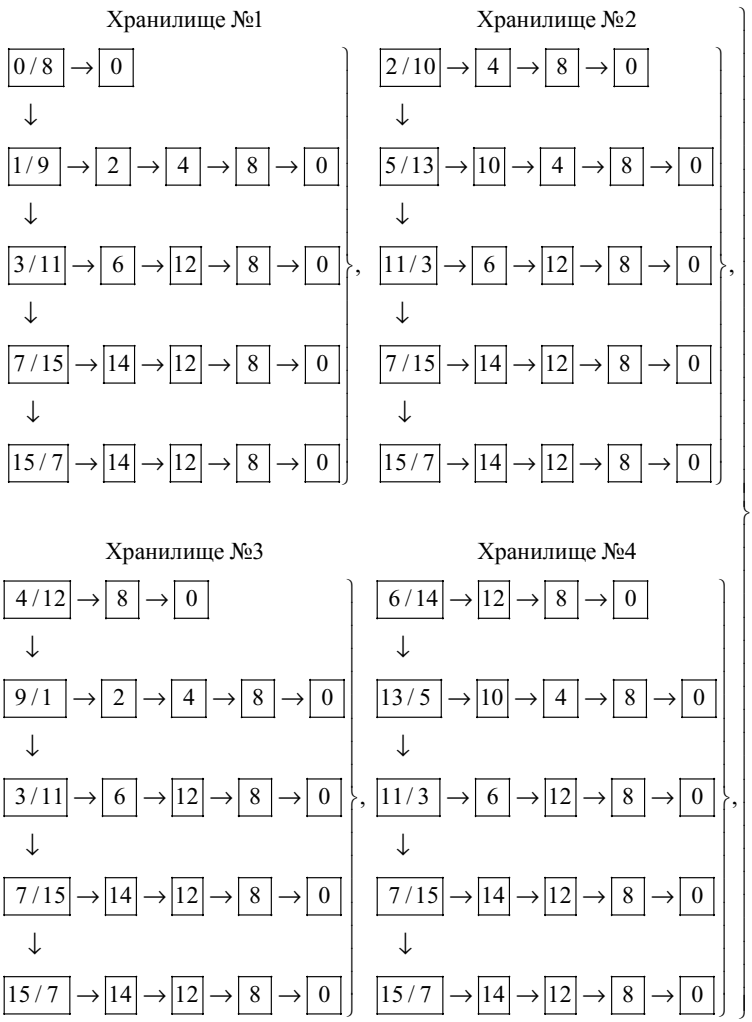
Построение ансамблей линейных и нелинейных Mg-последовательностей, максимального периода $N = 2^k$ сводится к реализации метода двойного сцепления: сцепления между векторами (для формирования всех кортежей векторов в рамках каждого хранилища) и между хранилищами (для сцепления подходящих кортежей), при этом в каждое хранилище нужно входить только один раз.

Выбранный на данной итерации кортеж векторов назовем подходящим, если он заканчивается одним из образующих векторов другого хранилища.

Для краткости и большей наглядности изложения материала каждый вектор A_i представим своим номером i.

Технические детали конструктивного метода построения Mg-последовательностей со свойством k-граммного распределения, представим в виде шагов с конкретными примерами:

Шаг 1.1. Для заданного значения k построить $p = 2^{k-2}$ хранилищ кортежей векторов. Например, для $k = 4$ соответствующие множества кортежей и хранилища представлены в виде сформированной на основе операторов $S0$ и $S1$ алгебраической конструкции



(4.4)

Шаг 1.2. В качестве первого хранилища для построения кортежей максимального периода N фиксируется Хранилище №1. Перебирая всяческие структуры кортежей и учитывая связи между хранилищами, можно найти множество опорных Q_i-последовательностей, каждая из которых имеет максимальный период $N=16$ (табл. 4.1).

Таблица 4.1

Множество Q-последовательностей

Q_i	Элементы Q_i-последовательности, $N=16$															
Q_1	0	1	2	4	9	3	6	13	10	5	11	7	15	14	12	8
Q_2	0	1	2	4	9	3	7	15	14	13	10	5	11	6	12	8
Q_3	0	1	2	5	10	4	9	3	6	13	11	7	15	14	12	8
Q_4	0	1	2	5	10	4	9	3	7	15	14	13	11	6	12	8
Q_5	0	1	2	5	11	6	12	9	3	7	15	14	13	10	4	8
Q_6	0	1	2	5	11	6	13	10	4	9	3	7	15	14	12	8
Q_7	0	1	2	5	11	7	15	14	12	9	3	6	13	10	4	8
Q_8	0	1	2	5	11	7	15	14	13	10	4	9	3	6	12	8
Q_9	0	1	3	6	12	9	2	5	11	7	15	14	13	10	4	8
Q_{10}	0	1	3	6	13	10	4	9	2	5	11	7	15	14	12	8
Q_{11}	0	1	3	6	13	10	5	11	7	15	14	12	9	2	4	8
Q_{12}	0	1	3	6	13	11	7	15	14	12	9	2	5	10	4	8
Q_{13}	0	1	3	7	15	14	12	9	2	5	11	6	13	10	4	8
Q_{14}	0	1	3	7	15	14	13	10	4	9	2	5	11	6	12	8
Q_{15}	0	1	3	7	15	14	13	10	5	11	6	12	9	2	4	8
Q_{16}	0	1	3	7	15	14	13	11	6	12	9	2	5	10	4	8

Другие последовательности могут быть получены путем всех циклических сдвигов каждой образующей Q_i-последовательности .

Шаг 1.3. Согласно системе (4.2) строится полное множество Mg_j - последовательностей, $j=\overline{1,256}$, линейных и нелинейных.

Например, на основе данных табл. 4.1 строится в возрастающем порядке множество всех образующих Mg_g-последовательностей, $g=\overline{1,16}$, каждая со свойством k-граммного распределения, представленное в (4.5). Рядом с каждой Mg_g-последовательностью проставлен её десятичный эквивалент $(Mg_g)_{10}$ Линейные Mg_1 и Mg_{13}-последовательности, которые могут быть построены на базе m-последовательностей, отмечены жирным шрифтом своих десятичных эквивалентов.

$$G=\begin{bmatrix}
Mg_1 = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1], & (Mg_1)_{10} = \mathbf{2479} \\
Mg_2 = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1], & (Mg_2)_{10} = 2539 \\
Mg_3 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1], & (Mg_3)_{10} = 2671 \\
Mg_4 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1], & (Mg_4)_{10} = 2683 \\
Mg_5 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1], & (Mg_5)_{10} = 2877 \\
Mg_6 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1], & (Mg_6)_{10} = 2927 \\
Mg_7 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 1], & (Mg_7)_{10} = 3031 \\
Mg_8 = [0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1], & (Mg_8)_{10} = 3027 \\
Mg_9 = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 1], & (Mg_9)_{10} = 3261 \\
Mg_{10} = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1], & (Mg_{10})_{10} = 3375 \\
Mg_{11} = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1], & (Mg_{11})_{10} = 3449 \\
Mg_{12} = [0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1], & (Mg_{12})_{10} = 3557 \\
Mg_{13} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1], & (Mg_{13})_{10} = \mathbf{3885} \\
Mg_{14} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1], & (Mg_{14})_{10} = 3915 \\
Mg_{15} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1], & (Mg_{15})_{10} = 3929 \\
Mg_{16} = [0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1], & (Mg_{16})_{10} = 3941
\end{bmatrix}. \quad (4.5)$$

Уже при $k > 4$ Метод 1 довольно трудоемкий, поскольку, в сущности, сводится к перебору всех возможных комбинаций кортежей в хранилищах.

Для сокращения объема вычислений существует метод синтеза Mg-последовательностей, который учитывает их структурные свойства.

4.3 Метод синтеза последовательностей с k-граммным распределением на основе учета структурных свойств

Применение метода перебора всего множества не является приемлемым решением учитывая объем множества, который исследуется даже при сравнительно небольших значениях k. Для сокращения объема вычислений вводится тестирование текущей последовательности T_i, которая перебирается на соответствие структурным свойствам Mg-последовательностей.

Последовательность T_i представляется в виде десятичного числа — ее номера $(T_i)_{10}$, и в виде N–разрядного двоичного вектора $(T_i)_2 = \{t_{2^k}, t_{2^k-1}, ..., t_0\}$, то есть

$$T_i = (T_i)_{10} = (T_i)_2, \quad i = \overline{0, 2^{k-1} - 1}, \tag{4.6}$$

Причем вторая половина последовательностей из полного множества T_i, инверсна первой и перебор можно сократить в 2 раза, приняв $i = \overline{0, \left(2^N / 2\right)}$.

Полученные результаты на основе Метода 1 синтеза *Mg*-последовательностей позволяют сформулировать ряд общих свойств.

Свойство 1. Свойство сбалансированности. Для каждой *Mg*-последовательности выполняется свойство сбалансированности $K^{(1)} = K^{(0)} = N / 2$, где $K^{(1)}$ и $K^{(0)}$, соответственно, число символов "1" и число символов "0" на максимальном периоде N *Mg*-последовательности.

Свойство 2. Свойство k-граммного распределения. В последовательностях T_i, которые тестируются, должны содержаться блоки из нулей или из единиц размера не более чем $k \le \log_2 N$.

Свойство 3. Все образующие *Mg*-последовательности имеют нечетный десятичный эквивалент, вида

$$(Mg_{образующая})_{10} = 2\lambda + 1, \ \lambda \in \mathbb{Z} \tag{4.7}$$

и, таким образом, переменную цикла поиска i можно изменять с шагом $step = 2$.

Свойство 4. Десятичный эквивалент первой *Mg*-последовательности должен быть выше минимального значения номера

$$\left(T_{\min}\right)_{10} = 2^{N-k-1} + 2^{N-2k} + 1, \quad N = 2^k, \tag{4.8}$$

то есть перебор нужно начинать с минимального значения номера $\left(T_i\right)_{10} \ge \left(T_{\min}\right)_{10}$ последовательности T_i. Этот результат вытекает из утверждений Метода 1 синтеза на основе двойного сцепления кортежей.

Свойство 5. Десятичный эквивалент последней *Mg*-последовательности, которая тестируется должен быть меньше максимального значения номера

$$\left(T_{\max}\right)_{10} \le \left(T_{\min}\right)_{10} + 2^{N-k-1}, \qquad (4.9)$$

поскольку все Mg_i-последовательности, расположенные после данного десятичного эквивалента, будут совпадать с ранее найденными с точностью до циклического сдвига.

Структурные свойства двоичной (эквивалентной бинарной) последовательности часто описывают [85] с помощью количества блоков, которые входят в нее, где блок — последовательность одинаковых символов.

Свойство 6. Каждая Mg-последовательность содержит оптимальное количество блоков символов $\mu_{\text{opt}} = N/2$, которое согласно гипотезы Л.Е. Варакина [85] имеют только последовательности с незначительными пиками автокорреляционных функций.

На основании учета свойств 1…5 время перебора полного кода для поиска Mg-последовательностей со свойством k-граммного распределения может быть существенно сокращено.

4.4 Метод синтеза последовательностей с k-граммным распределением на основе целочисленных функций

В основе данного метода лежит эвристический подход к синтезу образующих Mg-последовательностей на основе свойств специальных целочисленных функций. В теории клеточных автоматов часто используется функция целочисленного аргумента вида $\xi(n) = \text{XOR}\{n, 2n\}$ [95], которая вычисляется как поэлементная сумма по модулю 2 двух чисел: n и $2n$, представленных своими двоичными векторами [96]. Поскольку десятичный эквивалент каждой образующей Mg-последовательности — число нечетное, то функция $\xi(n)$ допускает такую модификацию, чтобы она генерировала множество нечетных чисел, то есть имела вид

$$\psi(h) = \mathrm{XOR}\{2h+1, 2(2h+1)\}, \quad h = \overline{1, 2^k - 1}\ . \tag{4.10}$$

Проведенные исследования позволили установить, что область поиска десятичных эквивалентов на основе целочисленной функции сокращается в два раза, в сравнении с Методом 2, при этом в области поиска всегда содержатся все десятичные эквиваленты образующих *Mg* -последовательностей. На рис. 4.2. приведены столбцовые диаграммы целочисленной функции $\psi(h)$.

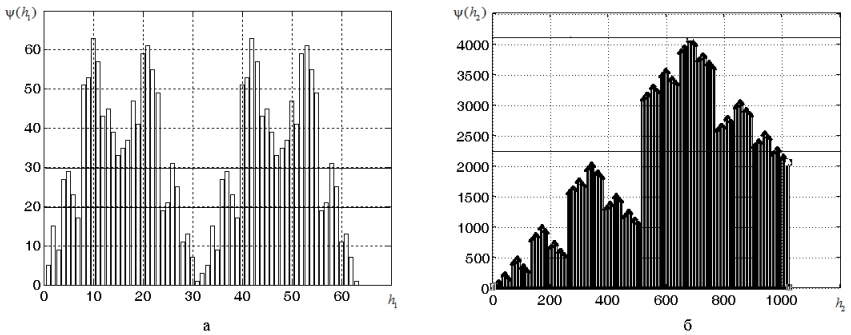


Рис. 4.2. Столбцовые диаграммы целочисленной функции:

$\psi(h_1) \bmod 2^6,\ h_1 = \overline{0,64}$ (а); $\psi(h_2) \bmod 2^{16},\ h_2 = \overline{0,1024}$ (б)

Алгоритм поиска *Mg* -последовательностей на основе целочисленной функции (4.11) по Методу 3, состоит из двух шагов:

Шаг 1. Для поиска всех образующих *Mg* -последовательностей по Методу 2 по известным минимальному и максимальному значениям номера $(T_{\min})_{10}$, $(T_{\max})_{10}$ необходимому и достаточному числу итераций $\Delta_2 = [(i_{\max})_{10} - (i_{\min})_{10}]/2$, найти границы изменения $h_{\min}$ и $h_{\max}$ переменной целочисленной функции (4.11) и число итераций для поиска этих же образующих *Mg* -последовательностей по Методу 3 из уравнений

$$i_{\min} = \psi(h_{\min}), \quad i_{\max} = \psi(h_{\max}), \quad \Delta_3 = h_{\max} - h_{\min}; \tag{4.11}$$

Шаг 2. Построить множество значений целочисленной функции $\psi(h)$ в диапазоне Δ_3 и отобрать методом проб значения, которые соответствуют десятичным эквивалентам *Mg* -последовательностей.

Проиллюстрируем приведенный метод синтеза конкретным примером, осуществив поиск образующих *Mg* -последовательностей длины $N = 16$ бит. По Методу 1 проведена оценка верхней и нижней границ области поиска *Mg* -последовательностей

$$\begin{cases} Mg_1 > \{00001001\ \ 00000001\}_2 = 2305_{10} = i_{\min}; \\ Mg_{16} < \{00001111\ \ 11111111\}_2 = 4095_{10} = i_{\max}. \end{cases} \quad (4.12)$$

Из соотношения (4.12) и данных рисунка 4.2 определяется $\Delta_3 = 959 - 512 = 450$ итераций. Получены значения аргументов h и целочисленной функции $\psi(h)$, соответствующие всему классу образующих *Mg* -последовательностей длины 16 бит (табл. 4.2).

Таблица 4.2

Соответствие значений целочисленной функции $\psi(h)$ класса *Mg* -последовательностей

Значение аргумента	h	565	593	619	626	653	657	667	668
Значение целочисленной функции	$\psi(h)$	3261	3557	3449	3375	3885	3941	3929	3915
Образующая *Mg* - последовательность	Mg_i	Mg_9	Mg_{12}	Mg_{11}	Mg_{10}	Mg_{13}	Mg_{16}	Mg_{15}	Mg_{14}
Значение аргумента	h	768	788	856	861	866	885	940	946
Значение целочисленной функции	$\psi(h)$	2671	2683	3027	3021	2895	2877	2539	2479
Образующая *Mg* - последовательность	Mg_i	Mg_3	Mg_4	Mg_8	Mg_7	Mg_6	Mg_5	Mg_2	Mg_1

4.5 Метод синтеза многоуровневых последовательностей с k-граммным распределением

Рассмотрим новый подход к решению проблемы синтеза полных классов многоуровневых Mg-последовательностей или последовательностей де Брейна (ПБ), сущность которого заключается в том, что каждая ПБ описывается с помощью двух форм: геометрической структуры и алгебраической структуры. На основе учета свойств этих структур предложен конструктивный метод синтеза полных классов многоуровневых ПБ. Далее рассматриваются вопросы применения построенных классов ПБ для конструирования экономичных схем S-блоков подстановки.

По определению каждая q-ичная последовательность де Брейна (ПБ), длины $N = q^k$, где q — основание ПБ, k-разрядность состояния (число ячеек памяти условного генератора) должна отображать на замкнутом цикле точно N разных между собой состояний. Например, если основание $q = 4$ (элементы $\{0,1,2,3\}$), а $k = 2$, то все $N = 4^2 = 16$ состояний ПБ разместим в $q = 4$ хранилищах и представим их в виде следующей алгебраической конструкции

Состояния	Хранилище	Состояния	Хранилище
[00] 01 02 03	№1	20 21 [22] 23	№3
10 [11] 12 13	№2	30 31 32 [33]	№4

. (4.13)

Конструкция (4.13) представляет собой довольно удобный объект для конструктивного построения разных множеств ПБ даже ручным способом. Состояния ПБ с одинаковыми числами в каждой из k ячеек памяти условно

назовем стационарными. В конструкции (4.13) стационарные состояния отмечены в прямоугольниках.

Определение 1. Геометрической структурой ПБ, длины $N = q^k$, назовем такой вектор $T = [\tau_1, \tau_2, \cdots, \tau_m]$, координаты τ_i которого определяют расстояния (число элементов) между каждыми двумя соседними стационарными состояниями на замкнутом цикле ПБ, при этом сумма координат вектора T

$$\sum_{i=1}^{q} \tau_i = q^k - qk . \tag{4.14}$$

Например, общий вид геометрической структуры произвольной ПБ, длины $N = 4^2 = 16$ на замкнутом цикле представим в виде следующей конструкции

$$00 \overset{\tau_1}{\longleftrightarrow} 11 \overset{\tau_2}{\longleftrightarrow} 22 \overset{\tau_3}{\longleftrightarrow} 33 \overset{\tau_4}{\longleftrightarrow} 00 , \tag{4.15}$$

которая определена с точностью до места и порядка расположения стационарных состояний.

Проведенные исследования позволили установить ряд свойств геометрических структур:

Утверждение 1. Полное множество геометрических структур объема $\Gamma_{\text{П}}$, всех ПБ, длины $N = q^k$, представляет собой все наборы векторов $T_i = \{\tau_{i,\kappa}\}$, $\kappa = \overline{1,q}$, каждый из которых удовлетворяет единственному ограничению (4.14), и так, полное множество геометрических структур строится конструктивно. Для ПБ, длины $N = 4^2 = 16$, находим $\Gamma_{\text{П}} = 165$.

Утверждение 2. Пусть заданная геометрическая структура $T_i = \{\tau_{i,\kappa}\}$, $\kappa = \overline{1,q}$, определяет подмножество ПБ объема J, тогда каждый циклический сдвиг и каждое не поглощенное циклическим сдвигом зеркальное отображение заданной структуры T_i определяет новое подмножество ПБ, такого же объема J, при этом новое подмножество ПБ нетрудно сформировать на основе прежде построенного подмножества ПБ.

Заметим, что для ряда геометрических структур операция циклического сдвига поглощает операцию зеркального отображения. Существуют также геометрические структуры с меньшим, чем q периодом цикличности. Определим эквивалентный класс геометрических структур как множество $\{T_i\}$, объема $J_{\text{экв}}$, полученных из заданной T_i, путем операций циклического сдвига и зеркального отображения. Очевидно, что каждый эквивалентный класс строится конструктивно. Выберем из каждого эквивалентного класса по одной геометрической структуре, в результате получим образующий класс геометрических структур, который обозначим через $\Gamma_{обр}$, а его объем $J_{обр}$. Для ПБ, длины $N = 4^2 = 16$, находим значение $\Gamma_{обр}$ и $J_{экв}$, которые представлены в табл. 4.3. Из анализа данных табл. 4.3 устанавливаем, что объем множества образующих структур $J_{утв} = 29$.

Таблица 4.3

Значения $\Gamma_{утв}$ и $J_{\text{екв}}$

$\Gamma_{обр}$	$J_{экв}$	$w_{обр}$	$\Gamma_{обр}$	$J_{экв}$	$w_{обр}$	$\Gamma_{обр}$	$J_{экв}$	$w_{обр}$
0008	4	216	0152	8	102	1115	4	36
0017	8	204	0161	4	72	1124	8	48
0026	8	162	0206	4	156	1133	4	60
0035	8	186	0215	8	120	1214	4	72
0044	4	192	0224	8	126	1223	8	66
0107	4	144	0233	8	114	1313	2	24
0116	8	114	0305	4	192	0323	4	156
0125	8	126	0241	4	168	1232	4	120
0134	8	96	0404	2	120	2222	1	96
0143	8	150	0314	8	138	–	–	–

Каждый фиксированный вектор T_i при фиксированном порядке следования стационарных состояний определяет собой подмножество точно из $w_{обр}$ ПБ (табл.4.3). Рассмотрим этот вопрос более полно. Методика и пример конструктивного построения подмножеств ПБ, объема $w_{обр}$, машинным или ручным способом, состоит в следующем:

Шаг 1. Выбираем вид геометрической структуры ПБ и фиксируем порядок стационарных состояний. Например, пусть $T_1 = [0,0,0,8]$, а порядок стационарных состояний — $[0,0,1,1,2,2,3,3]$.

Шаг 2. Представляем конструктивно каждую ПБ в виде объединения двух ее частей: стационарной части и, связывающего стационарную часть кортежа, длины (4.14). В нашем примере получаем следующую структуру: $\text{ПБ}_1 = [0,0,1,1,2,2,3,3,\text{кортеж}]$, в других случаях кортеж может быть распределенным, то есть вложенным в стационарную часть.

Шаг 3. Построим первый подходящий кортеж длины (4.14), начиная с наименьших подходящих элементов из диапазона $\{0,1,2,\cdots,m-1\}$, при которых выполняется свойство серий ПБ. Здесь довольно удобно воспользоваться вспомогательной алгебраической конструкцией (4.13), где, переходя от хранилища к хранилищу, будут сформированы все N состояний ПБ, а все тупиковые кортежи будут отброшены по ходу их появления. Теперь легко получаем, что в нашем примере $\text{ПБ}_1 = [0,0,1,1,2,2,3,3,0,2,0,3,1,3,2,1]$. Нетрудно убедиться, что на замкнутом цикле ПБ_1 наблюдается точно $N = 16$ разных между собой состояний. Продолжая построение других кортежей, устанавливаем, что при фиксированной геометрической структуре $T_1 = [0,0,0,8]$ и фиксированном порядке следования стационарных состояний — $[0,0,1,1,2,2,3,3]$ существует точно 36 ПБ, которые представлены в табл.4.4.

Таблица 4.4

Mg -последовательности при геометрической структуре $T_1 = [0,0,0,8]$

0011223302031321	0011223303213102	0011223313032021	0011223320302131
0011223302032131	0011223310203213	0011223313032102	0011223320310213
0011223302103132	0011223310213032	0011223313202103	0011223320313021
0011223302131032	0011223310213203	0011223313203021	0011223321020313
0011223302132031	0011223310302132	0011223313210203	0011223321031302
0011223303102132	0011223310320213	0011223313210302	0011223321302031
0011223303132021	0011223310321302	0011223320210313	0011223321303102
0011223303132102	0011223313020321	0011223320213031	0011223321310203
0011223303202131	0011223313021032	0011223320213103	0011223321310302

На основе найденных 36 ПБ (табл. 4.4), нетрудно построить точно по 36 новых структур ПБ для каждого из следующих пяти новых порядков следования стационарных состояний ПБ

$$\begin{bmatrix} 0,0,1,1,3,3,2,2 \\ 0,0,2,2,1,1,3,3 \\ 0,0,2,2,3,3,1,1 \\ 0,0,3,3,1,1,2,2 \\ 0,0,3,3,2,2,1,1 \end{bmatrix}. \qquad (4.16)$$

Итак, при фиксированном векторе $T_1 = [0,0,0,8]$ и фиксированном вначале ПБ нулевом стационарном состоянии, построены всего $w_{обр} = 6 \cdot 36 = 216$ образующих ПБ. Подобным образом найденные значения $w_{обр}$ (табл. 4.4) для всех других фиксированных векторов T_i при фиксированном в начале ПБ нулевом стационарном состоянии. На основе данных табл. 4.4 находим, что объем $W_{обр}$ образующего класса четверичных ПБ, длины $N = 4^2 = 16$ определяется соотношением

$$W_{обр} = \sum_{i=1}^{29} w_{\text{обр},i} J_{\text{обр},i} = 20736, \qquad (4.17)$$

что полностью отвечает существующей оценке существования объема образующего класса ПБ [72]

$$W_{обр} = [(q-1)!]^{q^k - 1} q^{q^{k-1} - k}. \qquad (4.18)$$

Для нахождения полного класса ПБ, на основе образующего класса ПБ, воспользуемся следующими свойствами ПБ:

Утверждение 3. Каждая образующая ПБ порождает, путем всех ее циклических сдвигов, точно $N = q^k$ ПБ из полного класса.

Утверждение 4. Полный класс ПБ имеет такое свойство, что операции циклических сдвигов образующих ПБ_i полностью поглощают операции

зеркального отображения образующих $ПБ_к$ для соответствующих пар чисел $(i, к)$.

На основе (4.17), с учетом содержания Утверждений 3 и 4, построим полный класс четверичных ПБ длины $N = 4^2 = 16$, и найдем его мощность

$$W_{полн} = NW_{обр} = 331776. \quad (4.19)$$

Рассмотрим процесс построения экономичных S-блоков подстановки на основе четверичных ПБ. Основным этапом построения S-блока подстановки является построение Q-последовательности. Для нахождения Q-последовательности воспользуемся свойством серий ПБ. Подробная процедура получения, например, десятичной $Q = [15,13,6,10,8,1,5,4,0,2,11,12,3,14,9,7]$ последовательности на базе четверичной $ПБ = [3,3,1,2,2,0,1,1,0,0,2,3,0,3,2,1]$, проиллюстрирована с помощью рис. 4.3 [97].

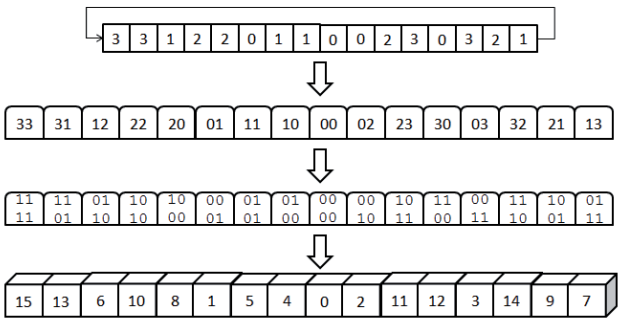


Рис. 4.3 — Получение Q-последовательности на основе четверичной ПБ

Анализ данных рис. 4.3 показывает, что применение четверичных ПБ позволяет добиться экономии памяти, необходимой для хранения S-блока в k раз. Так, в приведенном выше примере, для хранения десятичной Q-последовательности, необходимо 64 бита памяти, тогда как для хранения четверичной ПБ достаточно всего 32 бита.

4.6 Исследование криптографических свойств S-блоков подстановки на основе последовательностей со свойством k-граммного распределения

Согласно изложенному в первой главе материалу можем выделить следующие базовые критерии криптографического качества S-блоков подстановки:

1. Отсутствие корреляционной связи между входными и выходными битами S-блока. Для оценки данного критерия потребуем равномерность распределения элементов матрицы коэффициентов корреляции $|r_{\max}| \le 1/\eta$, где η – размерность компонентной функции S-блока.

2. Максимальное расстояние нелинейности, которое для сбалансированных функций не превышает значения $d_{S\max} \le 2^{\eta-1} - 2^{(\eta/2)-1} - 2$.

3. Максимальная длина циклов, на которые раскладывается подстановка, обусловленная как $T = HOK(i_1, i_2 ...)$, где i — соответствующие длины циклов.

4. Строгий лавинный критерий, определяемый через коэффициент распространения ошибки как $K_i(f) = \sum_{a_i} \left(f(x) \oplus f(x \oplus e_i) \right) = 2^{\eta-1}$.

Приведем табл. 4.7 [22,97…99], которая иллюстрирует значения вышеуказанных показателей криптографической устойчивости для разных классов Mg-последовательностей.

Таблица 4.7

Значение криптографически важных показателей S-блоков

Класс Mg – последовательностей	Объем класса $W = 2^{N/2}$	Количество J S-Блоков, которые обладают заданным параметром				Экономия памяти, раз
		$\lvert r_{\max}\rvert \le 1/\eta$	$d_S = 2^{\eta-1} - 2^{\frac{\eta}{2}-1} - 2$	T	$K_i(f) = 2^{\eta-1}$	
двоичные, $n=4$	256	24	192	21 ($T \ge 60$)	0	4
двоичные, $n=5$	65536	76	33032	1642 ($T \ge 1000$)	0	4
четверичные, $n=2$	331776	23008	218688	2281 ($T = 140$)	2176	2

Анализ данных табл.4.7 показывает высокую перспективность применения класса Mg-последовательностей для построения S-блоков подстановки современных экономичных криптографических систем.

ЗАКЛЮЧЕНИЕ

В настоящей работе представлены новейшие достижения в области синтеза одних из наиболее важных криптографических примитивов — S-блоков постановки, на базе которых построены практически все современные блочные симметричные криптографические алгоритмы.

В последние десятилетия произошел существенный прорыв в области разработки новых, более высококачественных S-блоков подстановки, в результате чего теория их синтеза вобрала в себя мощный математический аппарат теории булевых функций. Это позволило достаточно строго измерять криптографическое качество сконструированных S-блоков постановки как меру их резистивности тем или иным атакам криптоанализа. Данные криптографические критерии качества дали существенное развитие новым алгоритмам синтеза S-блоков подстановки с математически обоснованным уровнем криптографического качества.

Современные тенденции развития криптографических алгоритмов требуют дальнейшего развития двух ключевых характеристик S-блоков подстановки:

1. дальнейшего увеличения длины S-блока подстановки, что приводит к существенному улучшению его криптографических свойств;

2. увеличению числа синтезированных криптографически высококачественных S-блоков подстановки, что открывает возможности к использованию структуры S-блока подстановки в качестве долговременного ключевого элемента.

Тем не менее, уже разработанные современные методы синтеза S-блоков позволяют без существенных затрат (путем простой замены Q-последовательности) улучшить существующие криптографические системы, а также являются базисом для синтеза новых криптографических алгоритмов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Canright, D. A Very Compact S-Box for AES / D. Canright // LNCS 3659, Workshop on Cryptographic Hardware and Embedded Systems (CHES2005). — USA NY: Springer-Verlag. — P. 441—455. — 2005. — ISSN: 0302-9743.
2. Szaban, M. CA-based S-boxes for Secure Ciphers / M. Szaban, F. Seredynski. — Intelligent Information Systems. — Poland, Zakopane. — P. 99—110. — 2008. — ISBN: 978-83-60434-44-4.
3. Мазурков, М.И. Алгоритм синтеза оптимальных криптографических блоков подстановки на основе регулярных операторов децимации, перестановки и m–сдвига / М.И. Мазурков, В.Я. Чечельницкий, М.А. Мельник, А.В. Соколов // Одесса: Труды ОНПУ. — 2012. — С.179 — 187.
4. Schneier B. Applied Cryptography. 2-nd edition / B. Schneier — New York: John Wiley & Sons. — 1996.
5. Adams, C.M. Good S-boxes are easy to find / C.M. Adams, S.E. Tavares. — Advances in Cryptology: CRYPTO’89, Lect. Notes in Comput. Sci. — Vol. 435. — New-York: Springer-Verlag, 1990. — P. 612—615.
6. Beth, T. On almost perfect nonlinear permutations / T. Beth, C. Ding. — Advances in Cryptology: EUROCRYPT’93, Lect. Notes in Comput. Sci. — Vol.765. — New-York: Springer-Verlag, 1993. — P.65—76.
7. Webster, A. F. On the Design of S-Boxes / A.F Webster, S.E. Tavares. — Advances in Cryptology: CRYPTO'85/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 1986. — P. 523—534.
8. Gordon, J. Are big S-boxes best? / J. Gordon, H. Retkin. — Advances in Cryptology: EUROCRYPT'82/ Lect. Notes in Comput. Sei. — New York: Springer-Verlag. — 1983. — P. 257—262.
9. Kim, K. On generating cryptographically desirable substitutions / K. Kim, T. Matsumoto, H. Imai. — Transactions of the IEICE, E. — 1990. — Vol. 73. — 7. — P. 1031—1035.

10. Соколов, А.В. Конструктивный метод синтеза нелинейных S-блоков подстановки, соответствующих строгому лавинному критерию / А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2013. — Т. 56, N 8. — С. 43—52.

11. Мазурков, М.И. Синтез нелинейных преобразований на основе последовательностей де Брейна над изоморфными представлениями поля GF(256) / М.И. Мазурков, А.В. Соколов. — Одесса: Труды СИЭТ. —2013.— С. 208—211.

12. Логачев, О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. — М: Издательство МЦНМО. — 2004. — 472 с.

13. Сергиенко, Р.В. Исследование криптографических свойств нелинейных узлов замен алгоритма симметричного шифрования ГОСТ 28147-89 / Р.В. Сергиенко, И.В. Москвиченко // Харьковск. ун-т воздушн. сил им. Ивана Кожедуба, Системы обработки информации. — Харьков. — 2007. — №8(66). — С. 91—95.

14. Долгов, В.И. Исследование криптографических свойств нелинейных узлов замены уменьшенных версий некоторых шифров / В.И. Долгов, А.А. Кузнецов, И.В. Лисицкая, Р.В. Сергиенко // Радиотехника: Всеукр. межвед. науч-техн. сб. — Х. ХНУРЭ, 2008. — Вып. 136. — С. 131—139.

15. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Харків: Всеукраїнський міжвідомчий науково-технічний збірник "Радіотехніка". — 2004 . — Том 126. — С. 132—138.

16. Nyberg, K. Differentially uniform mappings for cryptography. In Advances in cryptology / K. Nyberg // Proc. of EUROCRYPT’93. — Berlin, Heidelberg, New York. — 1994. — vol.765, Lecture Notes in Compuer Springer-Verlag. — P.55 — 65.

17. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение / Б. Скляр. — Изд. 2-е, испр.: Пер. с англ. — М.: Издательский дом "Вильямс". — 2003. — 1104 с.

18. Limpaa, H. IDEA: A cipher for multimedia architectures / H. Limpaa. — Cryptography '98, volume 1556 of Lecture Notes in Computer Science. — Springer-Verlag, 1998. — P. 248 — 263.

19. Яковлєв, С.В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89 / Яковлєв С.В. // Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія». — 2009. — С. 5—12.

20. Горбенко, И.Д. Критерии отбора случайных таблиц подстановок для алгоритма шифрования по ГОСТ 28147-89 / И.Д. Горбенко, И.В. Лисицкая // Радиотехника: Всеукр. межвед. науч-техн. сб. — Харьков: ХНУРЭ. — 1997. — Вып. 103. — С. 121—130.

21. Ростовцев А. Г. Большие подстановки для программных шифров /А.Г. Ростовцев // Проблемы инф. безопасности. Компьютерные системы. — СПб.. — 2000. — № 3. — С. 31—34.

22. Мазурков, М.И. Методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения / М.И. Мазурков, А.В. Соколов. — Одесса: Труды ОНПУ. — 2012. — С.188 — 198.

23. Gao S. Design of bijective S-boxes satisfying the strict avalanche criterion / S. Gao, W. Ma, D. Shen // USA: Journal of computer information systems. — #6. — 2011. — P.1967—1973.

24. Kim K. A recursive construction method of S-boxes satisfying strict avalanche criterion / K. Kim, T. Matsumoto, H. Imai // Proc. of CRYPTO'90, Springer — Verlag. — 1990. — P.565—574.

25. Мазурков, М.И. Метод синтеза оптимальных подстановочных конструкций по критерию нулевой корреляции между выходными и входными

векторами данных / М. И. Мазурков // Известия высших учебных заведений. Радиоэлектроника. — 2012. — Т. 55, N 12. — С. 12—22.

26. Мазурков, М.И. Нелинейные преобразования на основе полных классов изоморфных и автоморфных представлений поля GF(256) / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2013. — Т. 56, N 11. — С. 16—24.

27. Соколов, А.В. Множество нелинейных преобразований на основе конструкции Ниберг длины N=256 / А.В. Соколов. — Одесса: Труды СИЭТ. — 2012.— С. 204—207.

28. Gao S. Improved hill-climbing methods in the design of bijective S-boxes. / S. Gao, W. Ma, J. Feng, N. Guo, Y. Yan // In proceeding of: Sixth International Conference on Natural Computation, ICNC 2010, Yantai, Shandong, China, 2010. — P. 2378—2380.

29. Казимиров, А.В. Выбор S-блоков для симметричных криптографических алгоритмов на основе анализа алгебраических свойств / А.В. Казимиров, Р.В. Олейников. — Вісник харківського національного університету, 2010. — №925. — С.79—86.

30. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/publications/

31. Cui, L A new S-box structure named affine-power-affine / L.Cui, Y. Cao. — International Journal of innovative computing, information and control, 2007. — Vol. 3. — No.3. — P.751—759.

32. Юкальчук, А.А. Критерии и показатели эффективности нелинейных преобразований симметричных криптоалгоритмов / А.А. Юкальчук. — Системи обробки інформації, 2006. — Вип. 3(52). — С. 186—190.

33. Государственный стандарт Союза ССР. Системы обработки информации. Криптографическая защита. Алгоритм криптографического преобразования ГОСТ 28147–89: — М.: ИПК Издательство Стандартов, 1990. — 28 с.

34. Лисицкая, И.В. Противоречивые подстановки в алгоритме ГОСТ 28147-89 / И.В. Лисицкая // Информационные системы: Сб. научн. тр. — Харьков: НАНУ, ПАНУ, ХВУ, 1995. — 9.с

35. Мазурков, М.И. Алгебраические свойства криптографических таблиц замен шифра Rijndael и шифра ГОСТ 28147-89 / М.И. Мазурков, А.В. Соколов. — Одесса: Труды СИЭТ. — 2012. — С.149.

36. Холоша, А.А. Об одном подходе к анализу качества блока подстановки битовых векторов / А.А. Холоша // Збірник наукових праць ІПМЕ НАН України. — Вип. 2. — Львів: Світ, 1998. — С.59—74.

37. Мухачев, В.А. Методы практической криптографии / В.А. Мухачев, В.А. Хорошко. — К.: ООО «Полиграф-Консалтинг», 2005. — 214 с.

38. Сачков, В. Н. Дискретные функции, используемые в криптографии / В.Н. Сачков, В.И. Солодовников, М.В. Федюкин. — М.: АК РФ, 1998. — 285 с.

39. Долгов, В.И. Подстановочные конструкции современных симметричных блочных шифров / Долгов В.И., Олейников Р.В., Лисицкая И.В., Сергиенко Р.В., Дроботько Е.В. Мельничук Е.Д. // Радіоелектронні і компютерні системи, ХНУРЭ. — 2009. — №6. — С.89—93.

40. Марченков С. С. Замкнутые классы булевых функций. — М.: Физматлит, 2000.

41. Мазурков, М. И. Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов / М. И. Мазурков, А. В. Соколов // Труды Одесского политехнического университета. — 2012. — №2(39). — С. 183–189.

42. Dawson, E Construction of correlation immune Boolean functions / E. Dawson, C.K. Wu // LNCS, 1997. — V. 1334. — P. 170—180.

43. Camion, P. Correlation immune and resilient functions over a finite alphabet and their applications in cryptography. — Design codes and cryptography, 1999. — Vol. 16. — No. 2. — P. 121—149.

44. Chee, S. On the correlation immune functions and their nonlinearity / S. Chee, S. Lee, D. Lee, S.H. Sung. — Advances in Cryptology: CRYPTO'85, Lect. Notes in Comput. Sci. — Vol. 218. — New-York: Springer-Verlag, 1986. — P.232—243.

45. Maitra, S. Autocorrelation properties of correlation immune Boolean funtions / S. Maitra. — Progress in cryptology: INDOCRYPT'2001, Lect. Notes in Comput. Sci. — Vol. 2247. — New-York: Springer-Verlag, 2001. — P. 242—253.

46. Maier W. Nonlinearity criteria for cryptographic functions / W.Maier, O.Staffelbach // In Advances in Cryptology — EUROCRYPT'89, vol.434, Lecture Notes in Computer Science, Springer-Verlag, 1990. — P.549-562.

47. Мак-Вильямс, Ф. Дж. Теория кодов исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. — М.: Связь, 1979. — 745 с.

48. Ростовцев, А.Г. Криптография и защита информации / А.Г. Ростовцев. — СПб.: Мир и Семья, 2002.

49. Мазурков, М.И. Регулярные привила построения полного класса бент-последовательностей длины 16 / М.И. Мазурков, А.В. Соколов // Труды ОНПУ. — 2013. — №2(41). — С.231—237.

50. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. — Томск, 2009. — Сер. №1(3). — С. 15—37.

51. Georgiou, S. Hadamard matrices, orthogonal designs and construction algorithms / S. Georgiou, C. Koukouvinos, J. Seberry. —Boston: Kluwer, 2003. — P. 133—205

52. McFarland, R.L. A family of difference sets in non-cyclic groups / R.L. McFarland // J. Combin. Theory. Ser. A. — 1973. — Vol. 15. — No. 1. — P. 1—10.

53. Мазурков, М.И. Системы широкополосной радиосвязи / М.И. Мазурков // Одесса: Наука и Техника. — 2010. — с. 340. — ISBN 978-966-8335-95-2.

54. Carlet, C. A construction of bent functions / C. Carlet. — Seventh joint Swedish-Russian international workshop on information theory. — St. Petersburg, Russia, 1995. — P. 57—59.

55. Nyberg K. Constructions of Bent Functions and Difference Sets / K. Nyberg. — Advances in Cryptology: EURO-CRYPT'90, Lect. Notes in Comput. Sci. — Vol. 473. — New York: Springer-Verlag. — 1991. — P. 151—160.

56. Nyberg K. New Bent Mappings Suitable for Fast Implementation / K. Nyberg. — Fast Software Encryption'93, Lect. Notes in Comput. Sci. — Vol. 809. — New York: Springer-Verlag. — 1994. — P. 179—184.

57. Savicky, P. On the bent Boolean functions that are symmetric / P. Savicky. — European Journal of Combinatorics. — 1994. — Vol. 15. — 4. — P. 407—410.

58. Yarlagadda, R., Hershey .I.E. Analysis and synthesis of bent sequences / R. Yarlagadda, I.E. Hershey. — Proc. IEE, Pt. E. — 1989. — Vol. 136. — 2. — P. 112—123.

59. Зайко, Ю.Н. Криптография глазами физика // Изв. Саратовского ун-та. — т. 9 вып. 2. — С. 34—48. — 2009.

60. Соколов, А.В. Периоды цикличности компактных S-блоков подстановки на основе последовательностей со свойством k–граммного распределения, Одесса: Труды СИЭТ. —2012. — С.150.

61. Lloyd, S.A. Characteristics and counting functions satisfying a higher order Strict Avalanche Criterion / S.A. Lloyd. — Advances in Cryptology: EUROCRYPT'89, Lect. Notes in Comput. Sci. — Vol. 434. — New-York: Springer-Verlag, 1990. — P.63—74.

62. Seberry, J. Improving the Strict Avalanche Characteristics of Cryptographic Functions / J. Seberry, X.M. Zhang, Y. Zheng. — Information Processing Letters. — 1994, — Vol. 50. — P. 37—41.

63. Szaban, M Cryptographically Strong S-Boxes Based on Cellular Automata / M. Szaban, F. Seredynski. — Polnad, Krakow: Lecture Notes in Computer Science, 2008. — Vol. 5191, P. 478—485.

64. Fuller, J Linear Redundancy in S-Boxes / J. Fuller, W. Millan. — Fast Software Encryption, 10th International Workshop, Sweden, Lund, 2003. — Vol. 2887. — P. 74—86.

65. Rothaus, O.S.: On “bent” functions / O.S. Rothaus // J. Comb. Theory Ser. A. — USA: Academic Press Inc, 1976. — №20(3). — P.300—305.

66. Carlet, C. An alternate characterization of the bentness of binary functions with uniqueness / C. Carlet, Ph. Guillot. — Design, Codes and Cryptography, 1998. — Vol. 14. — No.2. — P.33—140.

67. Мазурков, М.И. Метод защиты информации на основе совершенных двоичных решеток / М.И. Мазурков, В.Я. Чечельницкий, П. Мурр // Известия высших учебных заведений. Радиоэлектроника. — 2008. — Т. 51, N 11. — С. 53—57.

68. Wild, P. Infinite families of perfect binary arrays // P. Wild. — Electronics Letters (Volume:24 , Issue: 14). — United Kingdom, 1988. — P. 845—847.

69. Calabro, D On the synthesis of two-dimensional arrays with desirable correlation properties / D. Calabro and J. K. Wolf . — Inform. Contr. — Vol. 11. — P. 537—560. — p.1968.

70. Мазурков, М.И. Конструктивный метод синтеза полных классов многоуровневых последовательностей де Брейна / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2013. — Т. 56, N 1. — С. 43—49.

71. Hartke, S.G. Binary De Bruijn cycles under different equivalence relations / S.G. Hartke. — Discrete Mathematics, 2000. — No.215. — P.93—102.

72. De Bruijn N.G. A combinatorial problem // Nederl. Akad. Wetensch. Proc. — 1946. — V. 49. — P. 758—764.

73. Виноградов, И. М. Основы теории чисел / И.М. Виноградов. — М.: Наука, 1981.

74. Свердлик, М.Б. Оптимальные дискретные сигналы / Свердлик М.Б. – М.: Советское радио, 1975. — 200 с.

75. Шредер, М.Р. Числовые последовательности в физике, обработке сигналов и искусстве / М.Р. Шредер. — Акустический журнал, 2003. — Т.49. — №1. — С. 110—122.

76. J. Cock Toroidal tilings from de Bruijn-Good cyclic sequences / J.C. Cock. — Discrete Math., 70 (1988), P. 209—210.

77. Fan, C.T. On the Bruijn arrays / C.T Fan, S.M Fan, S.L Ma, M.K Siu. — Ars Combin., 19, 1985. — Vol. 19. — P. 205—213.

78. Hurlbert, G On the de Bruijn Torus problem / G. Hurlbert, G. Isaak // Journal of Combinatorial Theory, Series A. — Vol. 64, Issue 1, 1993. — P. 50—62.

79. Мазурков, М.И. Метод синтеза S-блоков по критерию нулевой корреляции между выходными и входными векторами данных и строгому лавинному критерию / М. И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2014. — Т. 57, N 8. — С. 54—60.

80. Kim, K. Construction of DES-like S-boxes Based on Boolean Functions Satisfying the SAC / K. Kim. — Proc. of Asiacrypt'91, Springer Verlag. — 1991. — P. 59—72.

81. Берлекэмп Э. Алгебраическая теория кодирования. — М: Издательство «МИР», 1971. — с. 477.

82. Мазурков, М.И. Эффективный алгоритм нахождения первообразных неприводимых полиномов / М.И. Мазурков, В.С. Дмитренко, Е.А. Конопака // Праці УНДІРТ. — Одесса. — 2005. — № 1. — С. 32—35.

83. Мазурков, М.И. Конструктивный способ построения первообразных полиномов над простыми полями Галуа / М.И. Мазурков. — Изв. вузов Радиоэлектроника. — 1999. — № 2. — С. 41—45.

84. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — Пер. с англ.: М.: Издательство ТРИУМФ, 2002 — 816 с.

85. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин.— М: Радио и связь, 1985. — 384 с.

86. OEIS. A002884 [Electronic resource]. — N. J. A. Sloane // http://oeis.org/A002884 .

87. Chandrasekharappa, T.G.S S-boxes generated using Affine Transformation giving Maximum Avalanche Effect / T.G.S. Chandrasekharappa, K.V. Prema, Kumara

Shama // Internation Journal of Computer Science and Engineering. — Manipal Institute of Technology, India. — Vol.3(#9). — 2011. — P.3185—3193.

88. Мазурков, М.И. Нелинейные S-блоки конструкции Ниберг с максимальным лавинным эффектом / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2014. — Т. 57, N 6. — С. 47—55.

89. Мазурков М.И. Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / Мазурков М.И., Конопака Е.А // Известия ВУЗов. Радиоэлектроника. — 2005. — № 11. — С. 58 — 65.

90. Мазурков, М.И. Нелинейные S-блоки подстановки на основе композиционных кодов степенных вычетов / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. — 2013. — Т. 56, N 9. — С. 34—43.

91. OEIS. A023689. — Olivier Gerard // http://oeis.org/A 023689.

92. Дворников, В.Д. Метод формирования бент-последовательностей / В.Д. Дворников. — Доклады БГУИР, Минск, 2003. — С. 106—109.

93. Knuth, D. The Art of Computer Programming. Vol. II. Seminumerical Algorithms / D. Knuth — USA, Commonwealth of Massachusetts: Addison-Wesley. — 1969. — p.634.

94. Мазурков, М.І. Основи теорії передавання інформації / М.І. Мазурков. — Одеса: Наука і техніка. — 2005. — 168 с.

95. OEIS. A048724 [Electronic resource]. — Antti Karttunen, 1999 // http://oeis.org/A048724 .

96. Гуров, С.И. Булевы алгебры, упорядоченные множества, решетки: Определения, свойства, примеры / С.И. Гуров. — М.: Либроком, 2013. — 352 с.

97. Соколов, А.В. Методы синтеза четверичных последовательностей де Брейна для задач криптографии / А.В. Соколов. — Материалы XVI

международной научной конференции: Решетнёвские чтения. — Красноярск. — 2012. — С. 682—683.

98. Мазурков, М.И. Автокорреляционные функции полного класса последовательностей со свойством k–граммного распределения / М.И. Мазурков, А.В. Соколов. — Одесса: Труды СИЭТ. — 2012. — С.148.

99. Соколов, А.В. Криптографические свойства экономичных S-блоков на основе последовательностей де Брёйна, Харьков: ММФ ХНУРЭ. — 2012. — С.195.