УДК 681.3.06

МАЗУРКОВ М.И., СОКОЛОВ А.В.

НЕЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ ПОЛНЫХ КЛАССОВ ИЗОМОРФНЫХ И АВТОМОРФНЫХ ПРЕДСТАВЛЕНИЙ ПОЛЯ $GF(256)$

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. Построен полный класс линейных рекуррентных последовательностей максимального периода (МЛРП) объема $\psi = 55296$, на основе всех автоморфных и изоморфных представлений основного поля $GF(256)$. Предложены конструкции S-блоков подстановки длины $N = 256$ на основе МЛРП, криптографические свойства которых не хуже свойств конструкции Ниберг шифра Rijndael. Общее число синтезируемых конструктивным методом подстановочных конструкций составляет $|S| = 7.4518 \cdot 10^{16}$, что делает возможным применение их в качестве долговременного ключа.

Abstract. The complete class of linear recurrent sequences of maximum period (MLRS) of volume $\psi = 55296$, on the basis of all automorphic and isomorphic representations of the main field $GF(256)$ is constructed. The construction of S-boxes of length $N = 256$ based on the MLRS, with cryptographic properties are not worse than those of Nyberg construction used in Rijdael cipher is proposed. The total number of constructively synthesized substitution structures is $|S| = 7.4518 \cdot 10^{16}$, which makes it possible to use them as long-term key.

Ключевые слова: S-блок подстановки, автоморфизм, изоморфизм, поля Галуа; substitution S-box, automorphism, isomorphism, Galois fields.

Базовым компонентом современных алгоритмов блочного шифрования, а также хеширования являются нелинейные S-блоки подстановки [1], которые осуществляют отображение группы входных битов x_i в другую группу выходных битов y_i по правилу, однозначно задаваемому кодирующей Q-последовательностью [2]. Применение для синтеза Q-последовательностей переборных методов является невозможным, т.к. уже при длине S-блока подстановки $N = 256$, число существующих Q-последовательностей достигает астрономического значения $J = 256! \approx 1{,}17 \cdot 10^{505}$. Вместе с тем при росте длины N существенно улучшаются корреляционные, дистанционные и криптографические свойства S-блоков подстановки, поэтому разработка конструктивных (не переборных) методов синтеза больших множеств кодирующих Q-последовательностей больших длин, является актуальной задачей.

Целью данной статьи является разработка конструктивного метода синтеза и исследование криптографических свойств однобайтовых S-блоков подстановки длины $N = 256$, построенных на основе полных классов изоморфных и автоморфных представлений поля $GF(256)$, с элементами в десятичной форме.

Основополагающая теорема полей Галуа гласит, что для каждого простого числа p и натурального n существует конечное алгебраическое поле порядка p^n, единственное с точностью до изоморфизма [3]. Однако заметим, что методы синтеза кодов, ансамблей шумоподобных сигналов, стоимость аппаратуры генерации и обработки кодов и сигналов существенно зависят от выбора вида представления поля. Поэтому с прикладной точки зрения целесообразно различные представления поля порядка p^n рассматривать как различные поля [4,5]. Для удобства изложения материала работы введем следующие обозначения и определения.

Величина $|f_q^k|$ — число первообразных полиномов $f(x)$ степени k над каждым изоморфным подполем $GF(q)$, которое определяется выражением $|f_q^k| = \varphi(q^k - 1)/k$, где

$\varphi(q^k-1)$ — фи-функция Эйлера. Величина $\left|\theta_q^k\right|$ — число первообразных корней в поле (подполе) $GF(q^k)$, которое определяется выражением $\left|\theta_q^k\right|=\varphi(q^k-1)$. Каждый первообразный полином $f(x)$ задает свою таблицу умножения, независимо от выбранного вида первообразного элемента $\theta\in GF(q^k)$. Произвольный i-ый элемент поля $GF(q^k)$, упорядоченного в соответствии с первообразным полиномом $f(x)$ степени k, представим в виде $\theta^i \bmod(f(x),q)=\alpha_{k-1}^{(i)}x^{k-1}+\alpha_{k-2}^{(i)}x^{k-2}+\cdots+\alpha_0^{(i)}$, $i=\overline{0,q^k-2}$, где коэффициенты $\alpha_\nu\in GF(q)$. Произвольный i-ый элемент десятичной линейной рекуррентной последовательности максимального периода (МЛРП) определяется соотношением

$$N_i=\sum_{\nu=1}^{k}\alpha_{k-\nu}^{(i)}q^{k-\nu},\quad i=\overline{0,q^k-2}. \tag{1}$$

Таким образом, структура десятичной МЛРП зависит как от вида первообразного полинома $f(x)$, так и от выбранного первообразного элемента $\theta\in GF(q^k)$.

Рассмотрим различные представления поля $GF(16)$, как поля $GF(2^4)$ и поля $GF(4^2)$, которые понадобятся в дальнейшем. Для упорядочения элементов поля $GF(2^4)$ выберем первообразный полином $f(x)=x^4+x+1$, неприводимый над полем $GF(2)$, и первообразный элемент $\theta=x\in GF(2^4)$. Соответственно, для поля $GF(4^2)$ выберем [6] первообразный полином $f(z)=z^2+z+3$, неприводимый над полем $GF(4)$, и первообразный корень $\theta=z\in GF(4^2)$. Перейдем к построению всех различных структур МЛРП с десятичной формой (1) представления элементов поля. В табл.1 построены упорядоченные элементы поля $GF(16)$ в различных форматах: в виде степеней первообразного элемента $\theta=x$, в виде полиномов над полем $GF(2)$, в виде двоичных векторов, в виде десятичных чисел, в виде степеней первообразного элемента $\theta=z$, в виде полиномов над полем $GF(4)$, в виде четверичных векторов, и снова в виде десятичных чисел

Таблица 1

Первообразный полином $f(x)=x^4+x+1$, над полем $GF(2)$				Первообразный полином $\psi(z)=z^2+z+3$, над полем $GF(4)$			
1	2	3	4	5	6	7	8
x^0	1	0001	1	z^0	1	01	1
x^1	x	0010	2	z^1	z	10	4
x^2	x^2	0100	4	z^2	$z+3$	13	7
x^3	x^3	1000	8	z^3	$2z+3$	23	11
x^4	$x+1$	0011	3	z^4	$z+1$	11	5
x^5	x^2+x	0110	6	z^5	3	03	3
x^6	x^3+x^2	1100	12	z^6	$3z$	30	12
x^7	x^3+x+1	1011	11	z^7	$3z+2$	32	14
x^8	x^2+1	0101	5	z^8	$z+2$	12	6
x^9	x^3+x	1010	10	z^9	$3z+3$	33	15
x^{10}	x^2+x+1	0111	7	z^{10}	2	02	2
x^{11}	x^3+x^2+x	1110	14	z^{11}	$2z$	20	8
x^{12}	x^3+x^2+x+1	1111	15	z^{12}	$2z+1$	21	9
x^{13}	x^3+x^2+1	1101	13	z^{13}	$3z+1$	31	13
x^{14}	x^3+1	1001	9	z^{14}	$2z+2$	22	10

Из анализа данных табл.1 нетрудно непосредственно убедиться в том, что структуры двух десятичных МЛРП (колонки 4 и 8) различны, поскольку различны правила их построения. Заметим, что для представления поля $GF(4) = GF(2^2) = \{0,1,2,3\}$ существует единственный первообразный полином $f(y) = y^2 + y + 1$, который полностью определяет таблицы сложения A и умножения M элементов этого поля:

$$A = \begin{array}{c|cccc} \oplus & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 0 & 3 & 2 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 2 & 1 & 0 \end{array}, \qquad M = \begin{array}{c|cccc} \otimes & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 2 & 3 \\ 2 & 0 & 2 & 3 & 1 \\ 3 & 0 & 3 & 1 & 2 \end{array}.$$

Конструктивные методы построения первообразных неприводимых над расширенными полями Галуа полиномов изложены, например, в [6].

Основное, рассматриваемое в данной работе поле $GF(256)$, имеет следующие свои изоморфные представления

$$GF(256) \Rightarrow GF(2^8) \Rightarrow GF(4^4) \Rightarrow GF(16^2). \qquad (2)$$

Для построения поля $GF(2^8)$ существуют $\left|f_2^8\right|$ полиномов и одно подполе $GF(2)$. Поэтому число изоморфных и автоморфных МЛРП определяется выражением $\psi_1 = \left|f_2^8\right| \cdot \left|\theta_2^8\right| = 16 \cdot 128 = 2048$. Для построения поля $GF(4^4)$ существуют $\left|f_4^4\right|$ первообразных полиномов и одно подполе $GF(4)$, поэтому число МЛРП определяется выражением $\psi_2 = \left|f_4^4\right| \cdot \left|\theta_4^4\right| = 32 \cdot 128 = 4096$. Для построения изоморфных полей вида $GF(16^2)$ существуют $\left|f_{16}^2\right|$ первообразных полиномов и $\left|f_2^4\right| + \left|f_4^2\right| = 2 + 4 = 6$ различных между собой изоморфных подполей $GF(16)$. Следовательно, количество МЛРП в данном случае определяется как $\psi_3 = \left[\left|f_2^4\right| + \left|f_4^2\right|\right] \cdot \left|f_{16}^2\right| \cdot \left|\theta_{16}^2\right| = 6 \cdot 64 \cdot 128 = 49152$. Полное количество десятичных МЛРП над всеми автоморфными и изоморфными полями (2) поля $GF(256)$ равно $\psi = \psi_1 + \psi_2 + \psi_3 = 55296$.

Приведенные выкладки позволяют сделать вывод о целесообразности использования различных изоморфных и автоморфных представлений основного поля $GF(256)$ для существенного увеличения количества различных структур МЛРП, на базе которых могут быть построены криптографические S-блоки подстановки.

Конструктивный метод построения криптографических S-блоков подстановки на основе изоморфных и автоморфных представлений основного поля $GF(256)$ изложим в виде следующих шагов:

Шаг 1. В соответствии с требуемым количеством S-блоков подстановки, а также требуемым уровнем их криптографического качества (см. табл. 3) выбираем представление основного поля $GF(256)$, так как $GF(2^8)$, $GF(4^4)$, $GF(16^2)$.

Шаг 2. В соответствии с конструктивным методом [6] строим первообразные неприводимые полиномы над выбранным на Шаге 1 расширением расширенного поля $GF(256)$.

Шаг 3. Выбираем первообразный элемент θ для которого в соответствии с выражением (1) строим элементы МЛРП N_i, $i = \overline{0, q^k - 2}$.

Шаг 4. На основе полученной последовательности МЛРП N_i формируем кодирующую Q-последовательность, полностью определяющую криптографический S-блок подста-

новки. Правило построение кодирующей Q-последовательности — конкатенация элементов МЛРП N_i с нулевым элементом поля

$$Q = [0 \mid \mathrm{N}_i], \tag{3}$$

где $\mid$ — символ горизонтальной конкатенации.

Заметим, что конкатенацию нулевого элемента поля с МЛРП можно осуществить $N-1=255$ различными способами, с практически одинаковыми (табл.3) криптографическими свойствами соответствующих S-блоков, получая при этом объем различных по структуре Q-последовательностей равный $|Q| = \psi \cdot (N-1) = 55296 \cdot 255 = 14100480$.

Приведем конкретный пример, иллюстрирующий работу конструктивного метода построения криптографических S-блоков подстановки на основе изоморфных и автоморфных представлений поля $GF(256)$.

Выберем например такое представление основного поля $GF(256)$, как $GF(4^4)$, над которым существует $\left|f_4^4\right| = 32$ первообразных полинома, один из которых

$$f(z) = z^4 + z^2 + 2z + 3. \tag{4}$$

Выберем первообразный элемент $\theta = z$, для которого в соответствии с (1) построим все элементы МЛРП N_i, после чего по правилу, определяемому (3) получаем все элементы кодирующей Q-последовательности, которые для краткости представим в шестнадцатеричном виде (табл. 2)

Таблица 2

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

Для исследования криптографических свойств построенных в соответствии с конструктивным правилом S-блоков подстановки примем следующие критерии качества их работы:

1. Минимальное значение максимального коэффициента $\min(\max\{r_{i,j}\})$ матрицы коэффициентов корреляции матрицы $R = \|r_{i,j}\|$, которая определяет степень линейной связи между векторами выхода y и входа x, S-блока подстановки, где коэффициенты корреляции

$$r_{i,j} = 1 - \frac{\sum_{m=1}^{N} (x_{m,i} \oplus y_{m,j})}{N/2},\ i, j = \overline{0, k-1}, \tag{5}$$

где $N = 2^k$ — длина двоичной булевой функции, символ $\oplus$ означает суммирование по $\bmod 2$.

Для примера (табл. 2), в соответствии с (5) матрица коэффициентов корреляции R имеет вид

$$R = \begin{bmatrix} 0.03125 & -0.015625 & -0.0625 & -0.03125 & 0.03125 & 0.03125 & 0.015625 & 0.015625 \\ 0.078125 & 0.09375 & 0.046875 & 0 & 0.078125 & -0.0625 & 0.078125 & -0.078125 \\ -0.09375 & 0 & 0.10938 & 0.0625 & 0 & 0.0625 & 0.0625 & -0.015625 \\ 0.09375 & 0.03125 & 0.015625 & -0.0625 & -0.015625 & 0.03125 & -0.015625 & 0.125 \\ 0.078125 & -0.09375 & 0.078125 & -0.09375 & 0.078125 & -0.09375 & 0.078125 & -0.09375 \\ -0.09375 & 0.078125 & -0.09375 & 0.078125 & -0.09375 & 0.078125 & -0.09375 & 0.078125 \\ -0.078125 & -0.046875 & 0.125 & -0.078125 & 0.0625 & -0.0625 & 0.0625 & -0.078125 \\ 0.09375 & 0.046875 & 0 & 0.078125 & -0.0625 & 0.078125 & -0.078125 & 0.078125 \end{bmatrix}, \tag{6}$$

тогда $\max\{r_{i,j}\} = 0.1250$, что свидетельствует о достаточно высоком качестве S-блока подстановки (табл. 2).

2. Количество K^0 нулевых значений матрицы коэффициентов корреляции: $r_{i,j} = 0$. Анализируя матрицу (6) нетрудно установить, что для S-блока подстановки (табл. 2) $K^0 = 4$.

3. Расстояние нелинейности S-блока подстановки — минимум расстояния Хэмминга между его компонентными булевыми функциями и всеми кодовыми словами аффинного кода [2,7]

$$N_S = \min\left\{\mathrm{dist}(F_i, \varphi_j)\right\},\ i = \overline{1,k},\ j = \overline{1, 2^{k+1}}, \tag{7}$$

где F_i — компонентные булевы функции, φ_j — кодовые слова аффинного $A(N,k)$–кода. Для примера (табл.2) нетрудно установить, что $N_s = 100$.

4. Алгебраическая степень нелинейности S-блока, определяемая как $\deg(S) = \min(\deg(F_i)), i = \overline{1,8}$, где $\deg(F_i)$ — число конъюнкций (степень) самого длинного слагаемого в полиноме Жегалкина (алгебраической нормальной форме) компонентной булевой функции F_i. Для S-блока подстановки (табл.2) $\deg(S) = 7$.

5. Период возврата S-блока в исходное состояние [8] — наименьшее общее кратное $T = \mathrm{НОК}(i_1, i_2 \ldots)$, где i — соответствующие длины циклов, на которые раскладывается подстановка Q. Для примера (табл.2), $T = 120$.

Проведенные с применением пакета прикладных программ для решения задач технических вычислений MATLAB исследования позволили систематизировать значения основных критериев криптографического качества при выборе различных параметров на *Шаге 1* и *Шаге 2* предложенного конструктивного метода построения S-блоков подстановки на основе пол-

ных классов изоморфных и автоморфных представлений поля $GF(256)$, которые в краткой форме представлены в табл. 3.

Таблица 3

Поле	Вид первообразного полинома	$\max\{r_{i,j}\}$	K^0	N_s	$\min\{\deg(F_i)\}$	T
1	2	3	4	5	6	7
$GF(2^8)$	все $\lvert f_2^8\rvert = 16$ первообразных полинома	0.1094…0.1250	1…10	96…106	6…7	74…17420
$GF(4^4)$	все $\lvert f_4^4\rvert = 32$ первообразных полинома	0.1094…0.1563	2…12	96…108	6…7	2…14060
$GF(16^2)$	$\{z^4+z+1\}$, {все $\lvert f_{16}^2\rvert = 64$ первообразных полинома}	0.0781…0.1563	1…17	96…106	7	2…80040
$GF(16^2)$	$\{z^4+z^3+1\}$, {все $\lvert f_{16}^2\rvert = 64$ первообразных полинома}	0.0781…0.1563	1…9	96…106	7	2…113050
$GF(16^2)$	$\{z^2+z+2\}$, {все $\lvert f_{16}^2\rvert = 64$ первообразных полинома}	0.1094…0.1563	1…12	96…106	7	2…10710
$GF(16^2)$	$\{z^2+z+3\}$, {все $\lvert f_{16}^2\rvert = 64$ первообразных полинома}	0.0938…0.1563	1…10	96…106	7	2…25872
$GF(16^2)$	$\{z^2+2\cdot z+2\}$, {все $\lvert f_{16}^2\rvert = 64$ первообразных полинома}	0.1094…0.1563	1…8	96…106	7	2…61503
$GF(16^2)$	$\{z^2+3\cdot z+3\}$, {все $\lvert f_{16}^2\rvert = 64$ первообразных полинома}	0.0938…0.1563	1…12	96…106	7	2…63140

Дальнейшее улучшение криптографического качества построенных конструктивно S-блоков подстановки на основе всех изоморфных и автоморфных представлений поля $GF(256)$ может быть достигнуто за счет применения на их выходе аффинных преобразований. Установлено, что всегда существует аффинное преобразование вида $y = Ax \oplus a$ [1], при котором период возврата T больше или равен периоду возврата S-блока шифра Rijndael. В криптографическом алгоритме Rijndael используется одно из таких аффинных преобразований вида

$$A=\begin{bmatrix}0&0&0&1&1&1&1&1\\0&0&1&1&1&1&1&0\\0&1&1&1&1&1&0&0\\1&1&1&1&1&0&0&0\\1&1&1&1&0&0&0&1\\1&1&1&0&0&0&1&1\\1&1&0&0&0&1&1&1\\1&0&0&0&1&1&1&1\end{bmatrix},\quad a=\begin{bmatrix}0\\1\\1\\0\\0\\0\\1\\1\end{bmatrix}, \tag{8}$$

которое существенно увеличивает период возврата конструкции Ниберг от величины $T=2$ до величины $T=1531530$.

Для S-блока подстановки (табл.2) даже методом подбора может быть найдена матрица аффинного преобразования

$$A=\begin{bmatrix}1&1&0&1&0&1&0&1\\1&1&1&0&0&0&0&0\\1&1&1&1&0&0&1&1\\0&0&1&1&0&1&1&1\\0&0&0&0&1&1&0&0\\0&1&1&1&0&1&0&1\\1&1&1&0&1&1&1&1\\0&1&0&0&1&0&0&0\end{bmatrix},\quad a=\begin{bmatrix}0\\0\\0\\0\\0\\0\\0\\0\end{bmatrix}, \tag{9}$$

увеличивающая период возврата разработанного конструктивно S-блока подстановки до $T=5\,356\,020$, что даже превосходит аналогичные показатели S-блока подстановки криптопреобразования Rijndael.

Дальнейшие исследования структурных свойств Q-последовательностей позволили установить, что мощность конструктивно построенного класса высококачественных S-блоков подстановки на основе всех изоморфных и автоморфных представлений поля $GF(256)$ может быть существенно увеличена с помощью следующего набора правил размножения:

— путем рассмотрения Q-последовательности как частотно-кодирующей последовательности (ЧКП), так и время-кодирующей последовательности (ВКП) [9], что позволяет удвоить их количество;

— путем осуществления N циклических сдвигов Q-последовательности, что позволяет получить из каждой кодирующей Q-последовательности еще N новых структур кодирующих Q-последовательностей;

— путем применения операции знакового кодирования а также перестановок компонентных булевых функций, как показано в [10], что позволяет получить из каждой кодирующей Q-последовательности еще $8!\cdot 2^8$ кодирующих Q-последовательностей.

Таким образом, с учетом всех приведенных правил, каждая Q-последовательность позволяет построить свое подмножество новых структур $\tilde{Q}$-последовательностей, объема $\left|\tilde{Q}\right|=2\cdot N\cdot 8!\cdot 2^8=5.2848\cdot 10^9$.

После данных преобразований нетрудно посчитать, что общий объем всех синтезируемых S-блоков подстановки определяется соотношением

$$\left|S\right|=\left|Q\right|\cdot\left|\tilde{Q}\right|=14100480\cdot 5.2848\cdot 10^9=7.4518\cdot 10^{16}. \tag{10}$$

Проведенный анализ полученных результатов исследований, аналогичный анализу, результаты которого приведены в табл.3 показал, что все выборочно исследованные S-блоки подстановки из объема (10) практически не уступают по показателям криптографического качества S-блокам подстановки конструкции Ниберг [10], которые применяются в криптографическом алгоритме Rijndael, однако их количество существенно превосходит количество S-блоков подстановки конструкции Ниберг.

ВЫВОДЫ

1. Получила дальнейшее развитие теория синтеза S-блоков подстановки на основе МЛРП, в рамках чего построен полный класс десятичных МЛРП объема $\psi = 55296$ над всеми изоморфными и автоморфными представлениями основного поля $GF(256)$. Предложена конструкция S-блока подстановки, основанная на кодирующей последовательности вида: $Q = [0 \,|\, \text{МЛРП}]$, и найдены конструктивные правила размножения кодирующих Q-последовательностей длины $N = 256$, общий объем которых $|S| = 7.4518 \cdot 10^{16}$.

2. Показано, что криптографические свойства построенных S-блоков подстановки не уступают по показателям криптографического качества S-блокам подстановки конструкции Ниберг, применяемым в криптографическом алгоритме Rijndael [10,7], однако имеют существенно больший объем, что делает возможным применение таких высококачественных S-блоков в качестве долговременного ключа.

3. Предложенный конструктивный метод синтеза однобайтовых S-блоков подстановки может быть использован при разработке больших процессорно-ориентированых нелинейных подстановок современных программных шифров [12], с разрядностью процессора $m = (16, 32, 64, 128)$.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Ростовцев А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко // СПб.: НПО «ПРОФЕССИОНАЛ». — 2004. — 478 с.

2. *Мазурков М.И.* Регулярный метод синтеза подстановочных криптографических конструкций с максимальным расстоянием нелинейности / М.И. Мазурков // Изв. вузов: Радиоэлектроника. — 2012. — Том 55. — № 3. — С. 29—36.

3. *Берлекэмп Э.Р.* Алгебраическая теория кодирования / Э.Р. *Берлекэмп* // М.: Мир, 1971. – 477с.

4. *Свердлик М.Б.* Оптимальные дискретные сигналы / М.Б. Свердлик //М.: Сов .радио, 1975. — 200с

5. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки: Пер. с англ / Р. *Блейхут* //М.: Мир, 1986. –576с.

6. *Мазурков М.И.* Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / Мазурков М.И., Конопака Е.А // Радиоэлектроника. — 2005. — № 11. — С. 58 — 65. (Изв. вузов).

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

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

9. *Мазурков М.И.* Системы широкополосной радиосвязи: учебное пособие для студентов высших учебных заведений / М.И. Мазурков // Одесса.: Наука и техника, 2010. — 340 с.

10. *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.

11. *Nyberg K.* Differentially uniform mappings for cryptography. I Advances in cryptology // Proceedings of EUROCRYPT'93 (1994) vol.765, Lecture Notes in Compuer Springer-Verlag, Berlin, Heidelberg, New York. P.55-65.

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

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