УДК 004.056.55

М.И. Мазурков, д-р техн. наук, проф.,
А.В. Соколов, бакалавр,
Одес. нац. политехн. ун-т

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА НЕЛИНЕЙНОГО ПРЕОБРАЗОВАНИЯ ШИФРА RIJNDAEL НА БАЗЕ ПОЛНЫХ КЛАССОВ НЕПРИВОДИМЫХ ПОЛИНОМОВ

М.І. Мазурков, А.В. Соколов. **Криптографічні властивості нелінійного перетворення шифру Rijndael на базі повних класів незвідних поліномів.** Розглянуті криптографічні властивості нелінійних блоків на основі зворотних щодо множення елементів над розширеними полями Галуа — конструкції Ніберг, що використається в шифрі Rijndael. Досліджено залежність криптографічних властивостей побудованих нелінійних блоків від виду використаного незвідного полінома, а також блочна структура їх компонентних булевих функцій. Розглянуто повний клас незвідних над полем Галуа $GF(2)$ поліномів степеня $k = 8$.

Ключові слова: нелінійне перетворення, незвідний поліном, шифрування, зворотний елемент, блокова структура.

М.И. Мазурков, А.В. Соколов. **Криптографические свойства нелинейного преобразования шифра Rijndael на базе полных классов неприводимых полиномов.** Рассмотрены криптографические свойства нелинейных блоков на основе обратных по умножению элементов над расширенными полями Галуа — конструкции Ниберг, использованной в шифре Rijndael. Исследована зависимость криптографических свойств построенных нелинейных блоков от вида использованного неприводимого полинома, а также блочная структура их компонентных булевых функций. Рассмотрен полный класс неприводимых над полем Галуа $GF(2)$ полиномов степени $k = 8$.

Ключевые слова: нелинейное преобразование, неприводимый полином, шифрование, обратный элемент, блочная структура.

M.I Mazurkov, A.V. Sokolov. **Cryptographic properties of nonlinear transform of Rijndael cipher based on complete classes of irreducible polynomials.** The properties of nonlinear cryptographic units based on the multiplicative inverse elements over extended Galois fields, also known as Nyberg construction used in Rijndael chipper are considered. The dependence of the cryptographic properties of the constructed nonlinear blocks upon the type of the used irreducible polynomial is investigated, as well as the block structure of their component Boolean functions. The full class of irreducible over $GF(2)$ field polynomials of degree $k = 8$ is considered.

Keywords: nonlinear transform, irreducible polynomial, encryption, inverse element, block structure.

Вне зависимости от выбранной архитектуры блочного симметричного шифра, например, сеть Фейстеля или *SP*-сеть, основным компонентом, определяющим устойчивость криптопреобразования к основным видам атак криптоанализа, является надежность нелинейного S-блока шифра [1]. Для построения S-блока шифра Rijndael/AES [2] выбрана за основу конструкция Ниберг, которая представляет собой отображение в виде мультипликативно обратных элементов поля Галуа $GF(2^k)$ [3]

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

скомбинированное вместе с аффинным преобразованием

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

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

A — невырожденная матрица аффинного преобразования;

a — вектор сдвига;

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

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

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

Из анализа (1) и (2) следует, что качество S-блока зависит от выбора вида неприводимого полинома $f(z)$ степени k из их полного множества $\mathbf{W}_k$, а также от выбора вида матрицы аффинного преобразования $\mathbf{A}$ из полного множества аффинных преобразований $\mathbf{W}_A$. Таким образом, нахождение вида полиномов $f(z)$ и соответствующего вида матриц аффинного преобразования $\mathbf{A}$, позволяющих получить S-блоки с наилучшими характеристиками, является актуальной задачей.

Предлагается исследование криптографических свойств нелинейных криптографических преобразований шифра Rijndael конструкции Ниберг, построенных на основе полных классов неприводимых полиномов и аффинных преобразований.

Для построения биективного нелинейного преобразования в соответствии с формулой (1) в качестве $f(z)$ возможно применение неприводимых, а также первообразных неприводимых полиномов [4]. Известно, что количество неприводимых q-ичных полиномов заданной степени k [5]

$$\left|\mathbf{W}_k\right| = \frac{1}{k}\sum_{\substack{d \\ d\,/k}} \mu(d)\, q^{(k/d)}\ , \tag{3}$$

где d — делители степени k;

$\mu(d)$ — функция Мебиуса;

запись d/k означает, что d делит k.

В этом множестве $\mathbf{W}_k$ количество первообразных полиномов

$$\left|\mathbf{V}_k\right| = \frac{\varphi(q^k-1)}{k}\ , \tag{4}$$

где $\varphi(x)$ — фи-функция Эйлера.

Например, для преобразования Rijndael $\left|\mathbf{W}_8\right| = 30$, $\left|\mathbf{V}_8\right| = 16$. В соответствии с конструктивными алгоритмами синтеза неприводимых полиномов [4] построим все неприводимые полиномы степени $k=8$ и представим их в виде десятичных эквивалентов

$$(f_i(z))_{10} = \left\{\begin{array}{l} 283,\ \mathbf{285},\ \mathbf{299},\ \mathbf{301},\ 313,\ 319,\ \mathbf{333},\ \mathbf{351},\ \mathbf{355},\ \mathbf{357},\ \mathbf{361},\ \mathbf{369},\ 375,\ 379, \\ \mathbf{391},\ 395,\ \mathbf{397},\ 415,\ 419,\ \mathbf{425},\ 433,\ 445,\ \mathbf{451},\ \mathbf{463},\ 471,\ 477,\ \mathbf{487},\ 499, \\ \mathbf{501},\ 505 \end{array}\right\}, \tag{5}$$

где жирным шрифтом выделены десятичные эквиваленты первообразных неприводимых полиномов.

Изучение зависимости криптографических характеристик преобразования Rijndael от вида неприводимого полинома включило в себя следующие оцениваемые параметры:

— Максимум коэффициента корреляции $\max\{r_{i,j}\}$ корреляционной матрицы $\mathbf{R}$, определяющей степень линейной связи между векторами выхода $\mathbf{y}$ и входа $\mathbf{x}$ S-блока подстановки для

$$r_{i,j} = 1 - \frac{\sum_{m=1}^{N}(x_{m,i} \oplus y_{m,j})}{N/2},\ i,j = \overline{0,k-1}, \tag{6}$$

где $N = 2^k$ — длина двоичной булевой функции;

символ $\oplus$ означает суммирование по $\mathrm{mod}\,2$.

Например, для полинома Rijndael

$$f_1(z) = z^8 + z^4 + z^3 + z + 1 = (100011011)_2 = (283)_{10} \tag{7}$$

матрица коэффициентов r_{ij} корреляции

$$\mathbf{R} = \begin{bmatrix} -0{,}0469 & 0{,}0625 & 0{,}0313 & -0{,}0156 & -0{,}0938 & -0{,}0156 & 0{,}0938 & -0{,}0938 \\ 0{,}0625 & 0{,}0938 & -0{,}0625 & -0{,}0938 & -0{,}1094 & 0{,}0156 & 0 & 0{,}0781 \\ 0{,}0313 & -0{,}0625 & -0{,}0938 & -0{,}0469 & 0{,}0156 & 0 & 0{,}0781 & 0{,}0625 \\ -0{,}0156 & -0{,}0938 & -0{,}0469 & -0{,}0625 & 0{,}0625 & -0{,}0625 & -0{,}0625 & 0{,}1250 \\ -0{,}0938 & -0{,}1094 & 0{,}0156 & 0{,}0625 & 0{,}0938 & 0{,}0469 & -0{,}0313 & -0{,}0156 \\ -0{,}0156 & 0{,}0156 & 0 & -0{,}0625 & 0{,}0469 & -0{,}0313 & -0{,}0156 & -0{,}0938 \\ 0{,}0938 & 0 & 0{,}0781 & -0{,}0625 & -0{,}0313 & -0{,}0156 & -0{,}0938 & -0{,}0156 \\ -0{,}0938 & 0{,}0781 & 0{,}0625 & 0{,}1250 & -0{,}0156 & -0{,}0938 & -0{,}0156 & 0{,}0938 \end{bmatrix}. \quad (8)$$

— Количество K^0 нулевых значений матрицы $\mathbf{R}$ коэффициентов корреляции, при $r_{ij} = 0$. Например, для полинома (7) в матрице (8) значение $K^0 = 4$.

— Расстояние нелинейности S-блока — минимум расстояния Хэмминга между его компонентными булевыми функциями и всеми кодовыми словами аффинного кода [1]

$$N_S = \min\{\mathrm{dist}(F_i, \varphi_j)\},\ i = \overline{1,k},\ j = \overline{1,2^{k+1}}, \quad (9)$$

где F_i — компонентная булева функция;

φ_j — кодовые слова аффинного $A(N,k)$ –кода.

— Количество μ блоков β в каждой компонентной булевой функции F_i, где блок определяется как последовательность из одинаковых символов [6]. Например, для нелинейного преобразования на базе полинома (7) находим количество блоков μ для каждой компонентной булевой функции (табл. 1).

Таблица 1

Количество блоков компонентных булевых функций нелинейного преобразования (7)

Компонентная функция F_i	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
Количество блоков μ	128	116	138	136	118	122	132	120

— Распределение длин $|\beta|$ блоков β, входящих в состав компонентных булевых функций F_i нелинейного преобразования. Для нелинейного преобразования на основе (7) матрица распределения длин блоков для каждой компонентной булевой функции F_i имеет вид

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

где первая строка содержит все возможные длины $|\beta|$ блоков. Очевидно, что в этом случае величина $|\beta|_{\max} = 11$.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Криптографические характеристики S-блоков на базе полного класса неприводимых полиномов (5), степени $k = 8$, $N = 256$, соответствующие оцениваемым критериям, приведены в табл. 2.

Таблица 2

Криптографические характеристики S-блоков на базе полного класса неприводимых полиномов (5), степени $n = 8$, $N = 256$

i	$(f_i(z))_{10}$	$\max\{r_{i,j}\}$	K^0	N_s	$\mu_{\min}...\mu_{\max}$	$\lvert\beta\rvert_{\max}$
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
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

Данные этой таблицы свидетельствуют о разнообразии выбора полиномов для использования в блочных шифрах в соответствии с решением использования того или иного критерия. Например, для обеспечения равномерной минимизации матрицы **R** коэффициентов корреляции целесообразнее всего использовать полиномы для обращения элементов с минимальным количеством K^0 нулей, например, $f_6 = 355$, $f_{29} = 499$. Применение данных полиномов позволит затруднить линейную аппроксимацию шифра аффинными булевыми функциями, увеличивая его сопротивляемость атакам дифференциального криптоанализа. Эти полиномы обладают лучшими (минимальными) значениями корреляции векторов выхода и входа S-блока подстановки по сравнению с полиномом (7), применяемым в алгоритме Rijndael.

Для обеспечения отсутствия корреляции векторов выхода и входа наиболее предпочтительными будут полиномы $f_{12} = 425$, $f_{18} = 313$. Они обладают наибольшим количеством нулей в матрицах $\mathbf{R}_i$ коэффициентов корреляции входа и выхода, 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, $i=\overline{1,8}$ обладают количеством блоков μ, близким к оптимальному значению $\mu_0 = N/2$, а также не содержат в своем составе слишком длинных последовательностей одинаковых символов, что позволяет говорить о высоком качестве автокорреляционных свойств функций F_i, в смысле малых значений их боковых лепестков [6].

Наряду с рассмотренными, другим важнейшим критерием криптографического качества функций F_i нелинейных преобразований является алгебраическая степень нелинейности $\deg(F_i)$, определяемая как степень самого длинного слагаемого функции, представленной в алгебраически нормальной форме, т.е. полиномов Жегалкина. Более высокая алгебраическая степень нелинейности $\deg(F_i)$ функций F_i позволяет противостоять атакам линейного криптоанализа, затрудняя аппроксимацию шифра системами линейных уравнений. Критерий максимизации алгебраической степени нелинейности можно модифицировать, потребовав, чтобы она для множества всех циклических сдвигов $\tau = \overline{0,255}$ функций F_i была константой

$$\psi = \{D^{\tau} F_i\}, \quad \tau = \overline{0, 2^k - 1}, \quad i = \overline{1,8}, \tag{11}$$

где D — оператор циклического сдвига.

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

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

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

Таким образом, для нелинейного преобразования на основе обратных элементов по модулю неприводимого полинома (7) для компонентных булевых функций F_2 и F_3 существуют такие значения циклических сдвигов τ, для которых алгебраическая степень нелинейности отличается от алгебраической степени нелинейности при $\tau = 0$.

Дальнейшие исследования позволили определить, что существуют такие неприводимые полиномы, для которых при любом значении циклического сдвига τ алгебраическая степень нелинейности $\deg(F_i)$ всех компонентных булевых функций нелинейного преобразования остается постоянной, т.е. $\deg(F_i) = 7$. Множество неприводимых полиномов в десятичном представлении, обладающих таким свойством,

$$\Omega = \{285, 351, 355, 463, 313, 319, 375, 379, 395, 415, 419, 433, 471, 477, 505\}. \tag{13}$$

Полиномы множества Ω обеспечивают свойство инвариантности алгебраической степени нелинейности компонентных булевых функций по отношению к циклическому сдвигу $\tau = \overline{0,255}$.

ISSN 2076-2429 (print)
ISSN 2223-3814 (on line)

Недостатком нелинейного преобразования (1) являются малые периоды цикличности T — возврата S-блока в исходное состояние, по построению $T = 2$. Возможность существенно увеличить периоды цикличности T лежит в использовании конструкции Ниберг (1), (2), включающей аффинное преобразования вида $\mathbf{b} = \mathbf{A} \cdot \mathbf{x} + \mathbf{a}$. Количество аффинных преобразований

$$\left|\mathbf{W}_A\right|_k = \prod_{i=0}^{k-1} (2^k - 2^i). \tag{14}$$

Например, для $k = 8$ $\left|\mathbf{W}_A\right|_8 \simeq 5{,}3 \cdot 10^{18}$ аффинных преобразований. В криптографическом алгоритме Rijndael используется одно из таких аффинных преобразований вида

$$\mathbf{A}_1 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad \mathbf{a} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}. \tag{15}$$

которое позволяет увеличить период цикличности нелинейного преобразования до величины $T_1 = 1\,531\,530$. Аффинное преобразование, увеличивающее периоды цикличности T нелинейного элемента, может быть подобрано индивидуально для каждого полинома так, что циклические свойства S-блока станут наилучшими. Например, матрица преобразования

$$\mathbf{A}_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}, \quad \mathbf{a} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tag{16}$$

позволяет получить период цикличности $T_2 = 14\,408\,856$ при работе с нелинейным элементом на основе (7).

Основные результаты проведенных исследований:

— исследованы криптографические свойства S-блоков подстановки конструкции Ниберг на базе полного класса неприводимых над полем Галуа $GF(2)$ полиномов степени $k = 8$, и показана возможность построения множества нелинейных S-блоков подстановки, обладающих привлекательными криптографическими свойствами: равномерной минимизацией матрицы коэффициентов корреляции, высокой степенью нелинейности по отношению к аппроксимации аффинными функциями, количеством блоков компонентных булевых функций F_i, близким к оптимальному, т.е. $\mu \simeq \mu_0$, небольшому значению размера $\left|\beta\right|_{\max}$ — максимальной длины последовательности одинаковых символов булевой функции;

— установлено, что период цикличности S-блоков конструкции Ниберг лежит в диапазоне $T_{\min} \ldots T_{\max} = 2 \ldots 14\,408\,856$, при этом период возврата реального S-блока шифра Rijndael можно увеличить, как минимум на порядок, путем выбора подходящего вида аффинного преобразования;

— исследованы структурные, корреляционные и дистанционные свойства компонентных булевых функций S-блоков, и, в частности, найдены такие неприводимые полиномы, для которых алгебраическая степень нелинейности компонентных булевых функций F_i инвариантна к циклическому сдвигу.

Литература

1. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Радіотехніка: всеукр. міжвідом. наук.-техн. зб. — Харків, 2004 . — Т. 126. — С. 132 — 138.
2. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/ publications/ — 03.10.2012
3. Nyberg, K. Differentially uniform mappings for cryptography. I 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.
4. Мазурков, М.И. Конструктивный способ построения первообразных полиномов над простыми полями Галуа / М.И. Мазурков // Изв. вузов Радиоэлектроника. — 1999. — № 2. — С. 41 — 45.
5. Берлекэмп, Э. Алгебраическая теория кодирования / Э. Берлекэмп. — М.: МИР, 1971. — 477 с.
6. Варакин, Л.Е. Системы связи с шумоподобными сигналами / Л.Е. Варакин. — М.: Радио и связь, 1985. — 384 с.

References

1. Horbenko, I.D. Doslidzhennia analitychnykh i statystychnykh vlastyvostei bulevykh funktsii kryptoalhorytmu RIJNDAEL (FIPS 197) [Investigation of analytical and statistical properties of Boolean functions of cryptographic algorithm RIJNDAEL (FIPS 197)] / I.D. Horbenko, O.V. Potii, Yu.A. Izbenko // Radiotekhnika: vseukr. mizhvidom. nauk.-tekhn. zb. [All-Ukrainian interdepartmental scientific and technical collection "Radio Engineering"] — Kharkiv, 2004. — Volume 126. — pp. 132 — 138.
2. FIPS 197. [Electronic resource] Advanced encryption standard. — 2001. — http://csrc.nist.gov/ publications/ — 03.10.2012
3. Nyberg, K. Differentially uniform mappings for cryptography. I Advances in cryptology / K. Nyberg // Proc. of EUROCRYPT'93. — Berlin, Heidelberg, New York. — 1994. — vol.765, Lecture Notes in Compuer Springer-Verlag. — pp.55 — 65.
4. Mazurkov, M.I. Konstruktivnyy sposob postroenia pervoobraznykh polinomov nad prostymi polyami Galua [Constructive method of primitive polynomials synthesis over prime Galois fields] / M.I. Mazurkov // Izv. vuzov Radioelektonika [News of the Universities: Radio Electronics]. — 1999. — # 2. — pp. 41 — 45.
5. Berlekehmp, A. Algebraicheskaya teoriya kodirovaniya [Algebraic coding theory] / A. Berlekehmp. — Moscow, 1971. — 477 pp.
6. Varakin, L.E. Sistemy svyazi s shumopodobnymi signalami [Communication systems with noise-like signals] / L.E. Varakin. — Moscow, 1985. — 384 pp.

Рецензент д-р техн. наук, проф. Одес. нац. политехн. ун-та Кобозева А.А.

Поступила в редакцию 1 ноября 2012 г.