УДК 004.056.55

ЭФФЕКТИВНЫЕ ВЫЧИСЛИТЕЛЬНЫЕ СХЕМЫ ДЛЯ АРИФМЕТИКИ ПОЛЯ ГАЛУА GF(2^8) В УСОВЕРШЕНСТВОВАННОМ СТАНДАРТЕ ШИФРОВАНИЯ

Рахман П.А.

ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Филиал в г. Стерлитамаке, e-mail: pavelar@yandex.ru

В рамках данной статьи рассматривается арифметика поля Галуа GF(2^8) на базе неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x + 1$, применяемого в усовершенствованном стандарте шифрования AES. Также рассматривается схема формирования таблиц степеней и логарифмов на базе примитивного элемента $\alpha = 3$, формулы сложения, умножения и деления, а также инвертирования элементов и возведения в заданную степень. Приводятся примеры выполнения арифметических операций с элементами поля. Также рассматриваются высокопроизводительные схемы прямого умножения и инвертирования элементов.

Ключевые слова: поле Галуа, арифметика, эффективные вычисления, стандарт шифрования

EFFECTIVE COMPUTATIONAL SCHEMES FOR THE ARITHMETIC OF GALOIS FIELD GF(2^8) IN THE ADVANCED ENCRYPTION STANDARD

Rahman P.A.

Ufa State Petroleum Technological University, Sterlitamak branch, e-mail: pavelar@yandex.ru

This paper deals with the arithmetic of Galois Field GF(2^8) based on the irreducible polynomial $p(x) = x^8 + x^4 + x^3 + x + 1$, which is used in the advanced encryption standard AES. The schemes for generating the tables of logarithms and anti-logarithms on base of the primitive element $\alpha = 3$, formula for the addition, multiplication, division, inversion of field elements and powering elements to the given degree are also discussed. Calculation examples of arithmetic operations with the field elements are also provided. The high-performance schemes of the direct multiplication and inversion of the field elements are also observed.

Keywords: Galois field, arithmetic, effective computations, advanced encryption standard

В настоящее время информация играет ключевую роль, как в жизни отдельного человека, так и в бизнес-процессах предприятий. Соответственно, защита ее от несанкционированного доступа в системах хранения и каналах передачи данных при помощи технологии шифрования данных является достаточно актуальной задачей [1]. Однако, современные стандарты шифрования данных [2] базируются на специализированных разделах математики, в частности, арифметике поля Галуа $GF(2^8)$, и для разработки программных или аппаратных реализаций, требуются дополнительные исследования [3-8] и выведение достаточно простых для понимания, и в то же время, высокопроизводительных вычислительных схем для конкретных стандартов шифрования информации.

Арифметика поля Галуа $GF(2^8)$ с применением логарифмов в стандарте шифрования данных AES. Поле Галуа $GF(2^8)$ является частным случаем расширенных конечных полей $GF(2^m)$ характеристики 2 и имеет широкое применение не только в помехоустойчивом кодировании информации, но и криптографии для защиты информации.

В частности, широко распространенное поле Галуа $GF(2^8)$ используется в стандарте AES – Advanced Encryption Standard (усовершенствованный стандарт шифрования).

Поле Галуа $GF(2^8)$ по определению содержит 256 элементов:

$GF(2^8)$:	$a(x)$:	0	1	x	…	$x^7+x^6+x^5+x^4+x^3+x^2+x+1$
	$(a)_2$:	00000000	00000001	00000010	…	11111111
	$(a)_{10}$:	0	1	2	…	255

Поле Галуа $GF(2^8)$, по определению являющееся полем многочленов вида $a(x) = a_7x^7 + \ldots + a_1x + a_0$, образуется на базе простого поля Галуа $GF(2)$ и неприводимого многочлена 8-й степени. В стандарте шифрования AES используется неприводимый многочлен следующего вида:

$$p(x) = x^8 + x^4 + x^3 + x + 1. \qquad (1)$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	3	5	15	17	51	85	255	26	46	114	150	161	248	19	53
16	95	225	56	72	216	115	149	164	247	2	6	10	30	34	102	170
32	229	52	92	228	55	89	235	38	106	190	217	112	144	171	230	49
48	83	245	4	12	20	60	68	204	79	209	104	184	211	110	178	205
64	76	212	103	169	224	59	77	215	98	166	241	8	24	40	120	136
80	131	158	185	208	107	189	220	127	129	152	179	206	73	219	118	154
96	181	196	87	249	16	48	80	240	11	29	39	105	187	214	97	163
112	254	25	43	125	135	146	173	236	47	113	147	174	233	32	96	160
128	251	22	58	78	210	109	183	194	93	231	50	86	250	21	63	65
144	195	94	226	61	71	201	64	192	91	237	44	116	156	191	218	117
160	159	186	213	100	172	239	42	126	130	157	188	223	122	142	137	128
176	155	182	193	88	232	35	101	175	234	37	111	177	200	67	197	84
192	252	31	33	99	165	244	7	9	27	45	119	153	176	203	70	202
208	69	207	74	222	121	139	134	145	168	227	62	66	198	81	243	14
224	18	54	90	238	41	123	141	140	143	138	133	148	167	242	13	23
240	57	75	221	124	132	151	162	253	28	36	108	180	199	82	246	1

Рис. 1. Таблица степеней 3^k для поля Галуа $GF(2^8)$ для AES

В двоичном представлении неприводимый многочлен выглядит как $(p)_2 = 100011011$, а в десятичном представлении: $(p)_{10} = 283$.

Наименьшим примитивным элементом поля $GF(2^8)$ является элемент $\alpha(x) = x + 1$, и при помощи него можно получить все ненулевые элементы поля, и он применяется в стандарте шифрования AES. В двоичном представлении примитивный элемент поля выглядит как $(\alpha)_2 = 11$, а в десятичном представлении, соответственно, как $(\alpha)_{10} = 3$.

Для формирования таблицы степеней примитивного элемента $\alpha(x) = x + 1$ используется представленная ниже рекуррентная схема для случая поля Галуа $GF(2^8)$ с неприводимым многочленом $p(x) = x^8 + x^4 + x^3 + x + 1$.

Что касается таблицы логарифмов, то ее можно формировать параллельно с формированием таблицы степеней, используя десятичное представление степеней примитивного элемента в качестве индексов таблицы логарифмов.

В двоичном представлении элементов поля операцию умножения на $(\alpha)_2 = 11$ в поле Галуа $GF(2^8)$ можно свести к операции сдвига влево на один разряд и операции сложения («побитового» XOR), причем в случае если старший бит «предыдущей» степени был ненулевым, то еще выполняется «побитовый» XOR с двоичным эквивалентом $(p)_2 = 100011011$ неприводимого многочлена.

$$\begin{cases} k = 1 \ldots 2^8 - 2; \quad \alpha^0 = 1; \quad \log_\alpha(\alpha^0) = 0; \\ \alpha^k = \begin{cases} ((\alpha^{k-1} << 1) \oplus \alpha^{k-1}), \quad \alpha_7^{(k-1)} = 0; \\ ((\alpha^{k-1} << 1) \oplus \alpha^{k-1}) \oplus (100011011)_2, \quad \alpha_7^{(k-1)} = 1; \end{cases} \\ \log_\alpha(\alpha^k) = k. \end{cases} \tag{2}$$

Под выражением $((\alpha^{k-1} << 1) \oplus \alpha^{k-1})$ понимается сдвиг двоичного числа влево на один разряд с последующей операцией «побитового» XOR результата сдвига с самим числом. Под выражением $((\alpha^{k-1} << 1) \oplus \alpha^{k-1}) \oplus (100011011)_2$ понимается сдвиг двоичного числа влево на один разряд с последующей операцией «побитового» XOR результата сдвига с самим числом, с последующей операцией «побитового» XOR результата с двоичным эквивалентом неприводимого многочлена.

Примечание. Поскольку в десятичном виде примитивный элемент поля $GF(2^8)$ выглядит как $(\alpha)_{10} = 3$, то будем также обозначать k-ую степень примитивного элемента как 3^k, а логарифм от элемента a по основанию примитивного элемента как $\log_3 a$.

Ниже на рис. 1 (в виде матрицы 16 x 16) приведены степени примитивного элемента $(\alpha)_{10} = 3$ поля Галуа $GF(2^8)$, образованного при помощи неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x + 1$. Степени примитивного элемента для компактности приведены в десятичном представлении, и расположены построчно (по 16 в строке), начиная с 0-й степени, и заканчивая 255-й.

Примечание 1. Для того, чтобы выбрать в таблице требуемую степень 3^k, необходимо выбрать строку и столбец таким образом, чтобы сумма индексов строки и столбца (индексы строк приведены в левом заголовоч-

ном столбце серого цвета, индексы столбцов – в верхней заголовочной строке серого цвета) была равна показателю степени k.

Также ниже на рис. 2 (в виде матрицы 16 х 16) приведены логарифмы по основанию примитивного элемента $(\alpha)_{10} = 3$ поля $GF(2^8)$. Логарифмы расположены построчно (по 16 в строке) для всех элементов поля, начиная с $(a)_{10} = 0$, заканчивая $(a)_{10} = 255$. Заметим, что логарифм от 0 не существует (соответствующая ячейка «N/A»).

Примечание 2. Для того, чтобы выбрать в таблице логарифм $\log_3 a$ заданного элемента a поля $GF(2^8)$, необходимо выбрать строку и столбец таким образом, чтобы сумма индексов строки и столбца (индексы строк приведены в левом заголовочном столбце серого цвета, индексы столбцов – в верхней заголовочной строке серого цвета) была равна десятичному представлению (эквиваленту) элемента a.

Тогда с учетом всего вышесказанного имеем арифметику поля Галуа $GF(2^8)$, образованного с помощью неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x + 1$ и на базе применения логарифмов по основанию примитивного элемента поля $(\alpha)_{10} = 3$:

- $\underbrace{a \pm b}_{GF(2^8)} = ((a_7 \oplus b_7)\ldots(a_0 \oplus b_0))_2 = a \oplus b.$

- $$\overbrace{a \cdot b}^{GF(2^8)} = \begin{cases} 3^{\overbrace{(\log_3 a + \log_3 b) \bmod (2^8 - 1)}^{< R, \{+, \cdot\} >}} & a \neq 0 \,\&\, b \neq 0; \\ 0 & a = 0 \vee b = 0. \end{cases} \quad (3)$$

- $$\overbrace{a / b}^{GF(2^8)} = \begin{cases} 3^{\overbrace{(\log_3 a + ((2^8 - 1) - \log_3 b)) \bmod (2^8 - 1)}^{< R, \{+, \cdot\} >}} & a \neq 0 \,\&\, b \neq 0; \\ 0 & a = 0 \,\&\, b \neq 0; \\ \textit{Ошибка} & b = 0. \end{cases}$$

Кроме того, если необходимо найти обратный элемент по умножению, то можно воспользоваться упрощенным вариантом формулы деления элементов:

- $$\overbrace{a^{-1}}^{GF(2^8)} = \begin{cases} 3^{\overbrace{((2^8 - 1) - \log_3 a) \bmod (2^8 - 1)}^{< R, \{+, \cdot\} >}} & a \neq 0; \\ \textit{Ошибка} & a = 0. \end{cases} \quad (4)$$

Наконец, для возведения в степень v заданного элемента a поля $GF(2^8)$ можно использовать формулу, применив операцию модулярного умножения логарифмов:

- $$\overbrace{a^v}^{GF(2^8)} = \begin{cases} 3^{\overbrace{(v \log_3 a) \bmod (2^8 - 1)}^{< R, \{+, \cdot\} >}} & a \neq 0 \,\&\, v \geq 0; \\ 0 & a = 0 \,\&\, v > 0; \\ 1 & a = 0 \,\&\, v = 0. \end{cases} \quad (5)$$

Пример 1. Найдем сумму элементов расширенного поля $GF(2^8)$, представленных в виде соответствующих чисел «87» и «131» в десятичной системе счисления. Имеем,

$$\underbrace{(87)_{10} + (131)_{10}}_{GF(2^8)} = \underbrace{(01010111)_2 + (10000011)_2}_{GF(2^8)} = \left\{ \begin{array}{c|c|c|c|c|c|c|c} \overset{0}{\oplus} & \overset{1}{\oplus} & \overset{0}{\oplus} & \overset{1}{\oplus} & \overset{0}{\oplus} & \overset{1}{\oplus} & \overset{1}{\oplus} & \overset{1}{\oplus} \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ \hline 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{array} \right\} =$$

$$= (11010100)_2 = (212)_{10}.$$

Таким образом, $\underbrace{(87)_{10} + (131)_{10}}_{GF(2^8)} = (212)_{10}$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	N/A	0	25	1	50	2	26	198	75	199	27	104	51	238	223	3
16	100	4	224	14	52	141	129	239	76	113	8	200	248	105	28	193
32	125	194	29	181	249	185	39	106	77	228	166	114	154	201	9	120
48	101	47	138	5	33	15	225	36	18	240	130	69	53	147	218	142
64	150	143	219	189	54	208	206	148	19	92	210	241	64	70	131	56
80	102	221	253	48	191	6	139	98	179	37	226	152	34	136	145	16
96	126	110	72	195	163	182	30	66	58	107	40	84	250	133	61	186
112	43	121	10	21	155	159	94	202	78	212	172	229	243	115	167	87
128	175	88	168	80	244	234	214	116	79	174	233	213	231	230	173	232
144	44	215	117	122	235	22	11	245	89	203	95	176	156	169	81	160
160	127	12	246	111	23	196	73	236	216	67	31	45	164	118	123	183
176	204	187	62	90	251	96	177	134	59	82	161	108	170	85	41	157
192	151	178	135	144	97	190	220	252	188	149	207	205	55	63	91	209
208	83	57	132	60	65	162	109	71	20	42	158	93	86	242	211	171
224	68	17	146	217	35	32	46	137	180	124	184	38	119	153	227	165
240	103	74	237	222	197	49	254	24	13	99	140	128	192	247	112	7

Рис. 2. Таблица логарифмов $\log_3 a$ для поля Галуа $GF(2^8)$для AES

Пример 2. Найдем произведение элементов поля $GF(2^8)$, представленных в виде соответствующих чисел «87» и «131» в десятичной системе счисления. По таблице логарифмов для поля $GF(2^8)$ имеем логарифмы элементов: $\log_3(87)_{10} = 98$ и $\log_3(131)_{10} = 80$. Тогда получаем:

$$\overbrace{(87)_{10} \cdot (131)_{10}}^{GF(2^8)} = 3^{\overbrace{(98+80)\bmod(255)}^{<R,\{+,\cdot\}>}} = 3^{178}.$$

По таблице степеней для поля $GF(2^8)$ имеем $3^{178} = (193)_{10}$. Таким образом:

$$\overbrace{(87)_{10} \cdot (131)_{10}}^{GF(2^8)} = (193)_{10}.$$

Пример 3. Найдем отношение элементов поля $GF(2^8)$, представленных в виде соответствующих чисел «131» и «193» в десятичной системе счисления. По таблице логарифмов для поля $GF(2^8)$ имеем логарифмы элементов: $\log_3(131)_{10} = 80$ и $\log_3(193)_{10} = 178$. Тогда получаем:

$$\overbrace{(131)_{10} / (193)_{10}}^{GF(2^8)} = \overbrace{3^{(80+(255-178))\bmod(255)}}^{<R,\{+,\cdot\}>} = 3^{157}.$$

По таблице степеней имеем $3^{157} = (191)_{10}$. Таким образом:

$$\overbrace{(131)_{10} / (193)_{10}}^{GF(2^8)} = (191)_{10}.$$

Пример 4. Найдем обратный элемент по умножению для элемента «191», представленного в десятичном виде. По таблице логарифмов имеем логарифм элемента: $\log_3(191)_{10} = 157$. Тогда обратный элемент:

$$\overbrace{((191)_{10})^{-1}}^{GF(2^8)} = 3^{\overbrace{(255-157)\bmod(255)}^{<R,\{+,\cdot\}>}} = 3^{98}.$$

По таблице степеней имеем $3^{98} = (87)_{10}$. Таким образом:

$$\overbrace{((191)_{10})^{-1}}^{GF(2^8)} = (87)_{10}.$$

Пример 5. Возведем элемент «13», представленный в десятичном виде, в заданную степень $v = 17$. По таблице логарифмов для поля $GF(2^8)$ имеем логарифм элемента: $\log_3(13)_{10} = 238$. Тогда по формуле получаем:

$$\overbrace{((13)_{10})^{17}}^{GF(2^8)} = 3^{\overbrace{(17\cdot 238)\bmod(255)}^{<R,\{+,\cdot\}>}} = 3^{221}.$$

По таблице степеней имеем $3^{221} = (81)_{10}$. Таким образом,

$$\overbrace{((13)_{10})^{17}}^{GF(2^8)} = (81)_{10}.$$

Схемы прямого умножение и инвертирование элементов поля Галуа $GF(2^8)$ в криптографическом стандарте AES. В случае необходимости высокопроизводительного прямого умножения элементов a и b поля Галуа $GF(2^8)$, можно использовать заранее подготовленную свертку многочленов $a(x)$ и $b(x)$ по модулю $p(x) = x^8 + x^4 + x^3 + x + 1$:

$$\underbrace{a \cdot b}_{GF(2^8)} = \underbrace{(a(x) \cdot b(x)) \bmod p(x)}_{GF(2)} = c_7 x^7 + c_6 x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0;$$

$$\begin{cases}
c_0 = a_0 \cdot b_0 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_6 \oplus a_3 \cdot b_5 \oplus a_4 \cdot b_4 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_6 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_1 \\
\quad \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_6; \\
c_1 = a_0 \cdot b_1 \oplus a_1 \cdot b_0 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_6 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_5 \oplus a_3 \cdot b_6 \oplus a_4 \cdot b_4 \oplus a_4 \cdot b_5 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_4 \\
\quad \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_6 \oplus a_7 \cdot b_1 \oplus a_7 \cdot b_2 \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_7; \\
c_2 = a_0 \cdot b_2 \oplus a_1 \cdot b_1 \oplus a_2 \cdot b_0 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_6 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_5 \oplus a_4 \cdot b_6 \oplus a_5 \cdot b_4 \oplus a_5 \cdot b_5 \oplus a_6 \cdot b_3 \\
\quad \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_2 \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_6; \\
c_3 = a_0 \cdot b_3 \oplus a_1 \cdot b_2 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_1 \oplus a_2 \cdot b_6 \oplus a_3 \cdot b_0 \oplus a_3 \cdot b_5 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_4 \oplus a_4 \cdot b_6 \oplus a_4 \cdot b_7 \\
\quad \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_5 \oplus a_5 \cdot b_6 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_5 \oplus a_6 \cdot b_6 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_1 \oplus a_7 \cdot b_3 \\
\quad \oplus a_7 \cdot b_4 \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_6 \oplus a_7 \cdot b_7; \\
c_4 = a_0 \cdot b_4 \oplus a_1 \cdot b_3 \oplus a_1 \cdot b_7 \oplus a_2 \cdot b_2 \oplus a_2 \cdot b_6 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_1 \oplus a_3 \cdot b_5 \oplus a_3 \cdot b_6 \oplus a_4 \cdot b_0 \oplus a_4 \cdot b_4 \\
\quad \oplus a_4 \cdot b_5 \oplus a_4 \cdot b_7 \oplus a_5 \cdot b_3 \oplus a_5 \cdot b_4 \oplus a_5 \cdot b_6 \oplus a_6 \cdot b_2 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_5 \oplus a_7 \cdot b_1 \oplus a_7 \cdot b_2 \oplus a_7 \cdot b_4 \\
\quad \oplus a_7 \cdot b_7; \\
c_5 = a_0 \cdot b_5 \oplus a_1 \cdot b_4 \oplus a_2 \cdot b_3 \oplus a_2 \cdot b_7 \oplus a_3 \cdot b_2 \oplus a_3 \cdot b_6 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_1 \oplus a_4 \cdot b_5 \oplus a_4 \cdot b_6 \oplus a_5 \cdot b_0 \\
\quad \oplus a_5 \cdot b_4 \oplus a_5 \cdot b_5 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_3 \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_6 \oplus a_7 \cdot b_2 \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_5; \\
c_6 = a_0 \cdot b_6 \oplus a_1 \cdot b_5 \oplus a_2 \cdot b_4 \oplus a_3 \cdot b_3 \oplus a_3 \cdot b_7 \oplus a_4 \cdot b_2 \oplus a_4 \cdot b_6 \oplus a_4 \cdot b_7 \oplus a_5 \cdot b_1 \oplus a_5 \cdot b_5 \oplus a_5 \cdot b_6 \\
\quad \oplus a_6 \cdot b_0 \oplus a_6 \cdot b_4 \oplus a_6 \cdot b_5 \oplus a_6 \cdot b_7 \oplus a_7 \cdot b_3 \oplus a_7 \cdot b_4 \oplus a_7 \cdot b_6; \\
c_7 = a_0 \cdot b_7 \oplus a_1 \cdot b_6 \oplus a_2 \cdot b_5 \oplus a_3 \cdot b_4 \oplus a_4 \cdot b_3 \oplus a_4 \cdot b_7 \oplus a_5 \cdot b_2 \oplus a_5 \cdot b_6 \oplus a_5 \cdot b_7 \oplus a_6 \cdot b_1 \oplus a_6 \cdot b_5 \\
\quad \oplus a_6 \cdot b_6 \oplus a_7 \cdot b_0 \oplus a_7 \cdot b_4 \oplus a_7 \cdot b_5 \oplus a_7 \cdot b_7.
\end{cases}$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	N/A	1	141	246	203	82	123	209	232	79	41	192	176	225	229	199
16	116	180	170	75	153	43	96	95	88	63	253	204	255	64	238	178
32	58	110	90	241	85	77	168	201	193	10	152	21	48	68	162	194
48	44	69	146	108	243	57	102	66	242	53	32	111	119	187	89	25
64	29	254	55	103	45	49	245	105	167	100	171	19	84	37	233	9
80	237	92	5	202	76	36	135	191	24	62	34	240	81	236	97	23
96	22	94	175	211	73	166	54	67	244	71	145	223	51	147	33	59
112	121	183	151	133	16	181	186	60	182	112	208	6	161	250	129	130
128	131	126	127	128	150	115	190	86	155	158	149	217	247	2	185	164
144	222	106	50	109	216	138	132	114	42	20	159	136	249	220	137	154
160	251	124	46	195	143	184	101	72	38	200	18	74	206	231	210	98
176	12	224	31	239	17	117	120	113	165	142	118	61	189	188	134	87
192	11	40	47	163	218	212	228	15	169	39	83	4	27	252	172	230
208	122	7	174	99	197	219	226	234	148	139	196	213	157	248	144	107
224	177	13	214	235	198	14	207	173	8	78	215	227	93	80	30	179
240	91	35	56	52	104	70	3	140	221	156	125	160	205	26	65	28

Рис. 3. Таблица обратных элементов по умножению для поля Галуа GF(2^8) для AES

Аппаратную реализацию схемы умножения мы не будем приводить в силу ее громоздкости. Отметим лишь, что ее несложно построить при помощи 64 двухвходовых логических элементов «И» и 8 многовходовых сумматоров по модулю 2.

Также в случае необходимости применения высокопроизводительного вычислителя обратного элемента по умножению (для ускорения операции деления), можно использовать заранее вычисленную таблицу обратных элементов по умножению.

Ниже на рис. 3 (в виде матрицы 16 х 16) приведены обратные элементы по умножению для элементов поля Галуа $GF(2^8)$, представленные в десятичном виде. Обрат-

ные элементы по умножению расположены построчно (по 16 в строке) для всех элементов поля, начиная с $(a)_{10} = 0$, заканчивая $(a)_{10} = 255$. Заметим, что обратного элемента по умножению для нуля не существует (соответствующая ячейка «N/A»).

Для аппаратной реализации таблицы можно использовать ПЗУ емкостью 256 х 8 бит.

Заключение

Таким образом, в рамках данной статьи рассмотрено поле Галуа $GF(2^8)$ на базе неприводимого многочлена $p(x) = x^8 + x^4 + x^3 + x + 1$, которое применяется в криптографическом стандарте AES (усовершенствованный стандарт шифрования). Также рассмотрены схема формирования таблиц степеней и логарифмов на базе примитивного элемента $(\alpha)_{10} = 3$, формулы сложения, умножения и деления, а также инвертирования элементов и возведения в заданную степень. Приведены примеры выполнения арифметических операций с элементами поля. Также рассмотрены высокопроизводительные схемы прямого умножения и инвертирования элементов поля.

Полученные результаты могут быть использованы при разработке эффективных программных и аппаратных реализаций вычислительных блоков в рамках шифрования и дешифрования информации по криптографическому стандарту AES.

Список литературы

1. Neal R.Wagner. The Laws of Cryptography with Java Code. University of Texas San Antonio, 2003.

2. Advanced Encryption Standard. FIPS PUB 197. National Institute of Standards and Technology, U.S. Department of Commerce, 2001.

3. Рахман П.А., Григорьева Т.В. Кодирование информации с применением кодов Рида-Соломона. – Уфа: Изд-во УГНТУ, 2015.

4. Рахман П.А. Алгоритм выбора кратности исправляемых искажений для кодирования информации с применением кодов Рида-Соломона // Международный журнал прикладных и фундаментальных исследований, 2015. – № 10-2. – С. 208–212.

5. Рахман П.А. Рекуррентный алгоритм вычисления формальной производной полинома над полем Галуа и его аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-1. – С. 14–18.

6. Рахман П.А. Рекуррентный алгоритм вычисления усеченной свертки полиномов над полем Галуа и его аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-2. – С. 231–235.

7. Рахман П.А. Арифметика поля Галуа на базе схемы сложения и вычитания логарифмов и ее аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-3. – С. 397–402.

8. Рахман П.А. Арифметика поля Галуа на базе быстрого умножения и инвертирования элементов поля и ее аппаратная реализация // Международный журнал прикладных и фундаментальных исследований, 2015. – № 12-3. – С. 403–408.