Кольца Илья С18-712: пример использования ранцевой криптосистемы в полях Галуа

Я решил взять за основу поле $GF(2^4)$ по модулю $q(x)=x^4+x^3+x^2+x+1$.

Тогда $(\lambda+1)^3,(\lambda+1)^2,(\lambda+1),(\lambda+1)^0$ возьмем в качестве базиса. Представим эти элементы в виде двоичных векторов, используя полученное выше представление через λ :

$(\lambda+1)^0=(0,0,0,1)$
$(\lambda+1)=(0,0,1,1)$
$(\lambda+1)^2=(0,1,0,1)$
$(\lambda+1)^3=(1,1,1,1)$

Перейдем к полю $GF(2^7)$.

Table B.26 Table of elements of GF(2^7){$x^7 + x + 1$}

$-\infty$:0000000	31:0001011	63:0001001	95:0100101
0:0000001	32:0010110	64:0010010	96:1001010
1:0000010	33:0101100	65:0100100	97:0010111
2:0000100	34:1011000	66:1001000	98:0101110
3:0001000	35:0110011	67:0010011	99:1011100
4:0010000	36:1100110	68:0100110	100:0111011
5:0100000	37:1001111	69:1001100	101:1110110
6:1000000	38:0011101	70:0011011	102:1101111
7:0000011	39:0111010	71:0110110	103:1011101
8:0000110	40:1110100	72:1101100	104:0111001
9:0001100	41:1101011	73:1011011	105:1110010
10:0011000	42:1010101	74:0110101	106:1100111
11:0110000	43:0101001	75:1101010	107:1001101
12:1100000	44:1010010	76:1010111	108:0011001
13:1000011	45:0100111	77:0101101	109:0110010
14:0000101	46:1001110	78:1011010	110:1100100
15:0001010	47:0011111	79:0110111	111:1001011
16:0010100	48:0111110	80:1101110	112:0010101
17:0101000	49:1111100	81:1011111	113:0101010
18:1010000	50:1111011	82:0111101	114:1010100
19:0100011	51:1110101	83:1111010	115:0101011
20:1000110	52:1101001	84:1110111	116:1010110
21:0001111	53:1010001	85:1101101	117:0101111
22:0011110	54:0100001	86:1001101	118:1011110
23:0111100	55:1000010	87:0110001	119:0111111
24:1111000	56:0000111	88:1100010	120:1111110
25:1110011	57:0001110	89:1000111	121:1111111
26:1100101	58:0011100	90:0001101	122:1111101
27:1001001	58:0111000	91:0011010	123:1111001
28:0010001	60:1110000	92:0110100	124:1110001
29:0100010	61:1100011	93:1101000	125:1100001
30:1000100	62:1000101	94:1010011	126:1000001

Пусть α - корень многочлена x^7+x+1 , т.е. α - примитивный элемент поля $GF(2^7)$.
Дополним наши базисные вектора до векторов длины 7 случайными битами:

$a_0=(1,0,|0,0,0,1|,1)=\alpha^{13}$
$a_1=(0,1,|0,0,1,1|,0)=\alpha^{68}$
$a_2=(0,0,|0,1,0,1|,0)=\alpha^{15}$
$a_3=(1,0,|1,1,1,1|,1)=\alpha^{81}$

В центре вертикальными чертами выделены исходные векторы
$(\lambda+1)^0,(\lambda+1)^1,(\lambda+1)^2,(\lambda+1)^3$.

Порядок мультипликативной группы поля $GF(2^7)$ равен 127. Разложим число 128 на 2 множителя, например 128 = 32 * 4. Для того, чтобы перейти от T_{easy} к $T_{shuffle}$, возведем векторы в степень, равную одному из делителей, например, в 4 степень.

Получим:

$b_0=a_0^4=(\alpha^{13})^4=\alpha^{52}=(1,1,0,1,0,0,1)$
$b_1=a_1^4=(\alpha^{68})^4=\alpha^{272\%127}=\alpha^{18}=(1,0,1,0,0,0,0)$
$b_2=a_2^4=(\alpha^{15})^4=\alpha^{60}=(1,1,1,0,0,0,0)$
$b_3=a_3^4=(\alpha^{81})^4=\alpha^{324\%127}=\alpha^{70}=(0,0,1,1,0,1,1)$

Пусть мы хотим передать сообщение $0,1,1,0$. Для этого нам необходимо сложить вектора a_1,a_2 и следовательно b_1,b_2 .

Получаем сообщение, складывая вектора по модулю 2 (xor):

1010000
1110000
0100000

Итоговое сообщение $c=(0,1,0,0,0,0,0)=\alpha^5$

Отправляем сообщение 2 участнику обмена сообщениями.

Участник возводит сообщение $c=(0,1,0,0,0,0,0)=\alpha^5$ в степень, равную 2 делителю, т.е. 32.

Получаем $c^{32}=(\alpha^5)^{32}=\alpha^{(160\%127)}=\alpha^{33}=(0,1,0,1,1,0,0)$.
Выбираем биты на соответствующих позициях $(0,1,|0,1,1,0|,0)$.

Получаем исходное сообщение $(0,1,1,0)$.