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

Я не совсем понял, как применять ранцевую систему не в десятичной системе счисления. Я решил взять за основу поле $GF(2^4)$ по модулю $q(x)=x^4+x^3+x^2+x+1$ (не является примитивным, можно было бы взять по модулю примитивного многочлена, но мне показалось, что тогда базис получается слишком простой).

Это поле я взял из своей работы по полям Галуа.

Пусть $\lambda \in GF(2^4)$ - корень неприводимого многочлена $q(x)$, над которым мы строим конечное поле $GF(2^4)$, т.е. $q(\lambda)=0$.
Попробуем построить поле, возводя в степень λ . Из того, что $q(\lambda)=0$, получаем $\lambda^4=\lambda^3+\lambda^2+\lambda+1$.

$\lambda^0=1$
$\lambda^1=\lambda$
$\lambda^2=\lambda^2$
$\lambda^3=\lambda^3$
$\lambda^4=\lambda^3+\lambda^2+\lambda+1$
$\lambda^5=\lambda^4+\lambda^3+\lambda^2+\lambda=\lambda^3+\lambda^2+\lambda+1+\lambda^3+\lambda^2+\lambda=2\lambda^3+2\lambda^2+2\lambda+1=1$

Получили, что корень λ порождает не все ненулевые элементы поля $GF(2^4)$, а только подмножество из 5 элементов.

Покажем, что элемент $\lambda+1$ порождает все поле $GF(2^4)$, не забывая, что $\lambda^4=\lambda^3+\lambda^2+\lambda+1$:

$(\lambda+1)^0=1$
$(\lambda+1)^1=\lambda+1$
$(\lambda+1)^2=\lambda^2+1$
$(\lambda+1)^3=(\lambda+1)(\lambda^2+1)=\lambda^3+\lambda^2+\lambda+1$
$(\lambda+1)^4=\lambda^4+1=\lambda^3+\lambda^2+\lambda+1+1=\lambda^3+\lambda^2+\lambda$
$(\lambda+1)^5=(\lambda+1)(\lambda^3+\lambda^2+\lambda)=\lambda^4+\lambda^3+\lambda^2+\lambda^3+\lambda^2+\lambda=\lambda^4+\lambda=\lambda^3+\lambda^2+1$
$(\lambda+1)^6=\lambda^6+\lambda^4+\lambda^2+1=\lambda+\lambda^3+\lambda^2+\lambda+1+\lambda^2+1=\lambda^3$
$(\lambda+1)^7=\lambda^4+\lambda^3=\lambda^3+\lambda^2+\lambda+1+\lambda^3=\lambda^2+\lambda+1$
$(\lambda+1)^8=\lambda^6+\lambda^4+\lambda^2=\lambda+\lambda^3+\lambda^2+\lambda+1+\lambda^2=\lambda^3+1$
$(\lambda+1)^9=\lambda^4+\lambda+\lambda^3+1=\lambda^3+\lambda^2+\lambda+1+\lambda+\lambda^3+1=\lambda^2$
$(\lambda+1)^{10}=\lambda^6+\lambda^4+1=\lambda+\lambda^3+\lambda^2+\lambda+1+1=\lambda^3+\lambda^2$
$(\lambda+1)^{11}=\lambda^4+\lambda^3+\lambda^3+\lambda^2=\lambda^3+\lambda+1$
$(\lambda+1)^{12}=\lambda^6=\lambda$
$(\lambda+1)^{13}=\lambda^2+\lambda$
$(\lambda+1)^{14}=\lambda^3+\lambda^2+\lambda^2+\lambda=\lambda^3+\lambda$
$(\lambda+1)^{15}=\lambda^4+\lambda^2+\lambda^3+\lambda=\lambda^3+\lambda^2+\lambda+1+\lambda^2+\lambda^3+\lambda=1$

Таким образом, поле $GF(2^4)$ построено по модулю неприводимого многочлена $q(x)=x^4+x^3+x^2+x+1$, но в степени возводился не корень этого многочлена λ , а элемент $\lambda+1$.

К*аждое число представимо в виде* $b_3(\lambda+1)^3+b_2(\lambda+1)^2+b_1(\lambda+1)+b_0$, $b_i \in GF(2), i=0..3$. 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 $GF(2^7)$. Я его сам не строил, нашел в интернете.

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

Для того, чтобы перейти от T_{easy} к $T_{shuffle}$, домножим каждый вектор на какой-нибудь заранее выбранный элемент поля $GF(2^7)$, например α^{75} .

Получим:

$b_0 = a_0 \alpha^{75} = \alpha^{13} \alpha^{75} = \alpha^{88} = (1,1,0,0,0,1,0)$

$b_1 = a_1 \alpha^{75} = \alpha^{68} \alpha^{75} = \alpha^{143\%127} = \alpha^{16} = (0,0,1,0,1,0,0)$

$b_2 = a_2 \alpha^{75} = \alpha^{15} \alpha^{75} = \alpha^{90} = (0,0,0,1,1,0,1)$

$b_3 = a_3 \alpha^{75} = \alpha^{81} \alpha^{75} = \alpha^{156\%127} = \alpha^{29} = (0,1,0,0,0,1,0)$

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):

0010100
0001101
0011001

Итоговое сообщение $c = (0,0,1,1,0,0,1) = \alpha^{108}$

Отправляем сообщение 2 участнику обмена сообщениями.

Участник 2 умножает сообщение $c = (0,0,1,1,0,0,1) = \alpha^{108}$ на мультипликативный обратный элемент к элементу α^{75} , который мы использовали ранее.

$(\alpha^{75})^{-1} = \alpha^{(127-75)} = \alpha^{52}$

Получаем $c * \alpha^{52} = \alpha^{108} \alpha^{52} = \alpha^{(160\%27)} = \alpha^{33} = (0,1,0,1,1,0,0)$.
Выбираем биты на соответствующих позициях $(0,1,|0,1,1,0|,0)$.

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

Я не уверен, что была необходимость использовать поле $GF(2^4)$. Также я не уверен, что умножение в поле — криптографически стойкая арифметическая операция.