

**S-BOX1** = [12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1]

**A. In field**  $cx^0 + ex^1 + 7x^2 + ex^3 + 5x^4 + 6x^5 + ax^6 + 7x^7 + 5x^8 + 7x^9 + cx^{10} + ex^{11} + 9x^{12} + 3x^{13} + bx^{14}$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
12	-8	10	-16	34	-77	169	-353
8	9	10	11	12	13	14	15
706	-1372	2635	-5076	9890	-19470	38383	-74890

Not Polinomial at index r = 4

**S-BOX2** = [6, 8, 2, 3, 9, 10, 5, 12, 1, 14, 4, 7, 11, 13, 0, 15]

**A. In field**

$f(x) = 6x^0 + cx^1 + 9x^2 + fx^3 + dx^4 + ax^5 + ex^6 + 3x^7 + bx^8 + 8x^9 + 5x^{10} + 3x^{11} + ex^{12} + 9x^{13} + cx^{14}$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
6	2	-8	15	-17	9	8	-15
8	9	10	11	12	13	14	15
-55	389	-1455	4335	-11361	27242	-60946	128762

Not Polinomial at index r = 3

**S-BOX3** = [11, 3, 5, 8, 2, 15, 10, 13, 14, 1, 7, 4, 12, 9, 6, 0]

$f(x) = bx^0 + bx^1 + bx^2 + 4x^3 + fx^4 + 3x^5 + 8x^6 + ex^7 + ax^8 + 2x^9 + ex^{10} + 6x^{11} + 1x^{12} + cx^{13} + bx^{14}$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
11	-8	10	-9	-1	39	-142	373
8	9	10	11	12	13	14	15
-831	1649	-2947	4679	-6265	5809	1461	-26182

Not Polinomial at index r = 3

**S-BOX4** = [12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11]

$f(x) = cx^0 + 8x^1 + ex^2 + 9x^3 + 1x^4 + 5x^5 + fx^6 + dx^7 + 8x^8 + 9x^9 + 4x^{10} + fx^{11} + 2x^{12} + 4x^{13} + 1x^{14}$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
12	-4	-2	7	1	-43	160	-433
8	9	10	11	12	13	14	15
1013	-2169	4379	-8521	16271	-30873	58473	-110114

Not Polinomial at index  $r = 3$

**S-BOX5** = [7, 15, 5, 10, 8, 1, 6, 13, 0, 9, 3, 14, 11, 4, 2, 12]

$$f(x) = 7x^0 + ax^1 + 2x^2 + dx^3 + 4x^4 + dx^5 + cx^6 + cx^7 + ex^8 + 9x^9 + 1x^{10} + 6x^{11} + bx^{12} + 5x^{13} + ax^{14}$$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
7	8	-18	33	-55	79	-88	55
8	9	10	11	12	13	14	15
35	-121	-77	1349	-5566	16767	-43144	100494

Not Polinomial at index  $r = 3$

**S-BOX6** = [5, 13, 15, 6, 9, 2, 12, 10, 11, 7, 8, 1, 4, 3, 14, 0]

$$f(x) = 5x^0 + 1x^1 + 0x^2 + 7x^3 + 5x^4 + fx^5 + 9x^6 + 1x^7 + 1x^8 + 9x^9 + 0x^{10} + 2x^{11} + 9x^{12} + 3x^{13} + cx^{14}$$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
5	8	-6	-5	28	-73	167	-366
8	9	10	11	12	13	14	15
770	-1546	2969	-5504	9983	-17994	32724	-60768

Not Polinomial at index  $r = 3$

**S-BOX7** = [8, 14, 2, 5, 6, 9, 1, 12, 15, 4, 11, 0, 13, 10, 3, 7]

$$f(x) = 8x^0 + 3x^1 + 3x^2 + 1x^3 + 6x^4 + 4x^5 + 3x^6 + ax^7 + 0x^8 + 1x^9 + cx^{10} + fx^{11} + 8x^{12} + 4x^{13} + 2x^{14}$$

**deg** = 14

**B. In Ring**

0	1	2	3	4	5	6	7
8	6	-18	33	-50	71	-109	207
8	9	10	11	12	13	14	15
-465	1061	-2234	4161	-6582	7867	-2925	-21122

Not Polinomial at index  $r = 3$

**S-BOX8** = [1, 7, 14, 13, 0, 5, 8, 3, 4, 15, 10, 6, 9, 12, 11, 2]

$$f(x) = 1x^0+9x^1+2x^2+5x^3+8x^4+2x^5+6x^6+1x^7+0x^8+7x^9+1x^{10}+6x^{11}+9x^{12}+1x^{13}+dx^{14}$$

**deg** = 14

### B. In Ring

0	1	2	3	4	5	6	7
1	6	1	-9	5	29	-113	261
8	9	10	11	12	13	14	15
-467	695	-899	1116	-1686	3651	-9367	23326

Not Polinomial at index r = 2