m =	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12	x13	x14	x15
m << 6	x6	x7	x8	x9	x10	x11	x12	x13	x14	x15	x0	x1	x2	x3	x4	x5
m << 10	x10	x11	x12	x13	x14	x15	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
c =	x0 x6 x10	x1 x7 x11	x2 x8 x12	x3 x9 x13	x4 x10 x14	x5 x11 x15	x6 x12 x0	x7 x13 x1	x8 x14 x2	x9 x15 x3	x10 x0 x4	x11 x1 x5	x12 x2 x6	x13 x3 x7	x14 x4 x8	x15 x5 x9
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
c << 10	x10 x0 x4	x11 x1 x5	x12 x2 x6	x13 x3 x7	x14 x4 x8	x15 x5 x9	x0 x6 x10	x1 x7 x11	x2 x8 x12	x3 x9 x13	x4 x10 x14	x5 x11 x15	x6 x12 x0	x7 x13 x1	x8 x14 x2	x9 x15 x3
C1 = c XOR (c<<10)	x6 x4	x7 x5	x8 x6	x9 x7	x10 x8	x11 x9	x12 x10	x13 x11	x14 x12	x15 x13	x0 x14	x1 x15	x2 x0	x3 x1	x4 x2	x5 x3
C2 = C1 << 2	x8 x6	x9 x7	x10 x8	x11 x9	x12 x10	x13 x11	x14 x12	x15 x13	x0 x14	x1 x15	x2 x0	x3 x1	x4 x2	x5 x3	x6 x4	x7 x5
C3 = C1 XOR C2	x8 x4	x9 x5	x10 x6	x11 x7	x12 x8	x13 x9	x14 x10	x15 x11	x0 x12	x1 x13	x2 x14	x3 x15	x4 x0	x5 x1	x6 x2	x7 x3
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
c << 14	x14 x4 x8	x15 x5 x9	x0 x6 x10	x1 x7 x11	x2 x8 x12	x3 x9 x13	x4 x10 x14	x5 x11 x15	x6 x12 x0	x7 x13 x1	x8 x14 x2	x9 x15 x3	x10 x0 x4	x11 x1 x5	x12 x2 x6	x13 x3 x7
C4 = C3 XOR (c << 14)	x14	x15	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12	x13
m = C4 << 2	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	x10	x11	x12	x13	x14	x15