Problem 13. «A present for you!»

Alice wants to implement the lightweight block cipher PRESENT on a chip. She starts with the bit permutation that is defined in Table and illustrated in Figure below. Clearly, many lines are intersecting, and this would cause a short circuit if the lines were metal wires. Is it possible to avoid this problem by using several “layers,” i.e., parallel planes? That is to draw the lines without intersections on each layer. We assume that

- the work area is a rectangle bounded by the lines where input and output bits are placed and the lines of the outermost connections $P(0) = 0$ and $P(63) = 63$;
- input and output bits are ordered; connections are represented by arbitrary curves;
- color of a line indicates the number of its layer, a line can change color several times;
- the point where a line changes color indicates a connection from one layer to another.

Q1 What is the minimun number of layers required for implementing in this way the PRESENT bit permutation?

Q2 Find a systematic approach how to draw a valid solution for the minimum number of layes found in **Q1** and present the drawing!

For your help (but not necessarily), you can use a specific online tool and download the PRESENT bit permutation as in Figure.

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P(i)$	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$P(i)$	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
$P(i)$	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$P(i)$	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Table: Definition of the bit permutation used in PRESENT.
Bit i is moved to bit position $P(i)$.

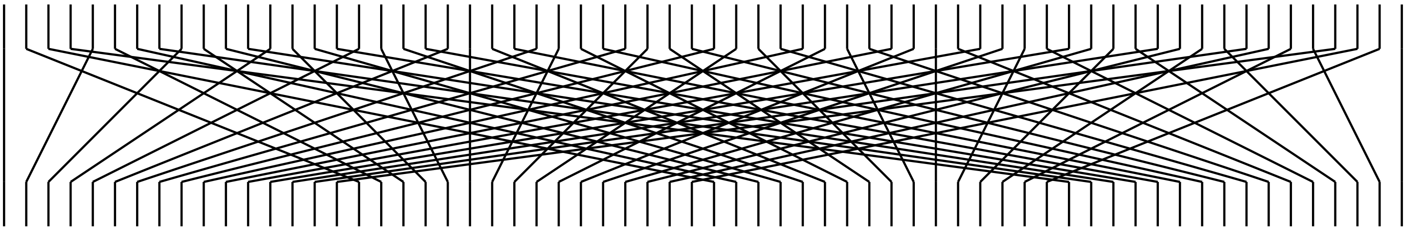

Figure: Illustration of the bit permutation used in PRESENT