DIGISIM PS-1

Team Name: The Hawks

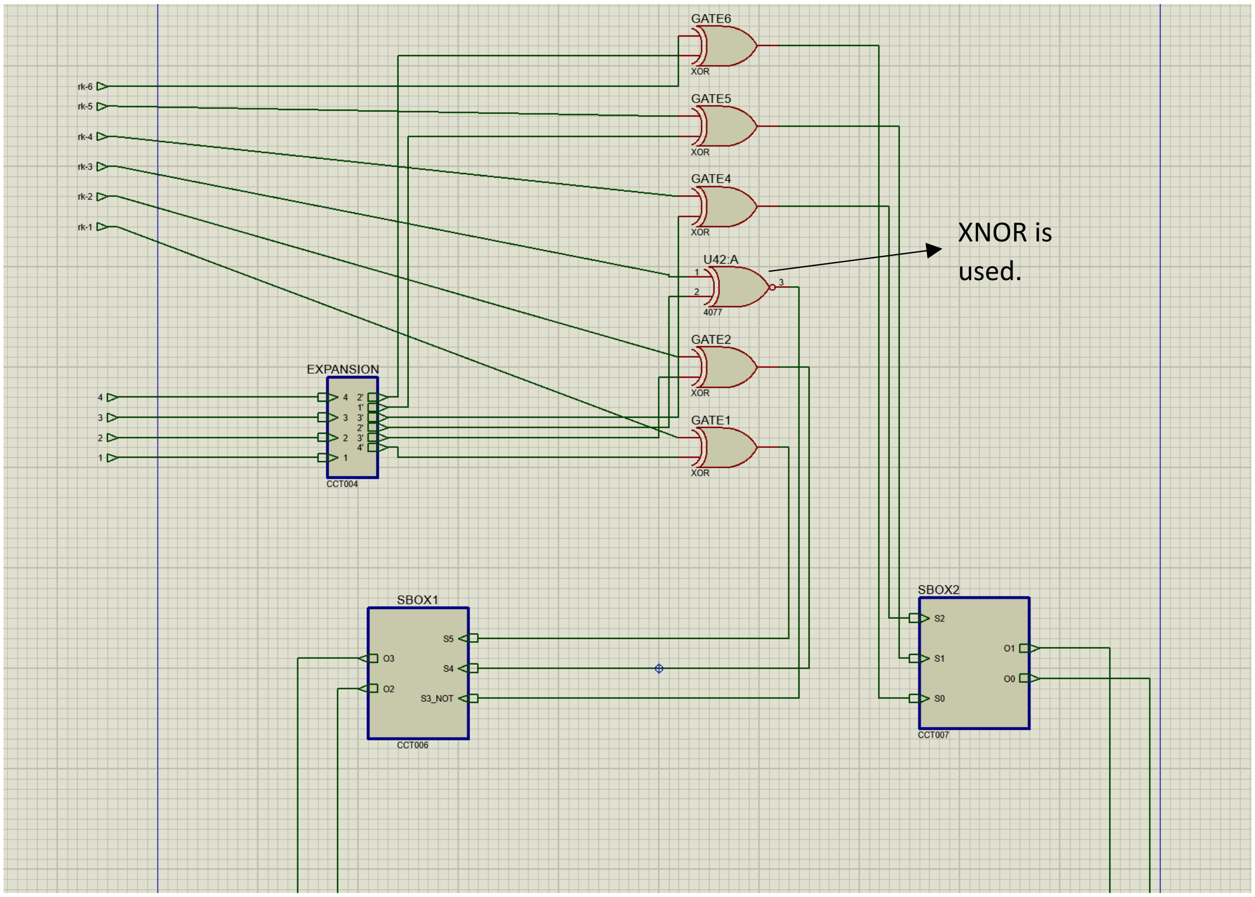
Combinational Circuit:

Part 1 (Encryption): **Total Cost = 8.4**

Permutation:

1. The permutation part of the circuit is inverse of the inverse permutation (i.e. if an inversely permuted data is permuted again, it yields the original data).
2. This part of the circuit was designed purely using wire rearrangement.

The f function: RK-1/RK-4

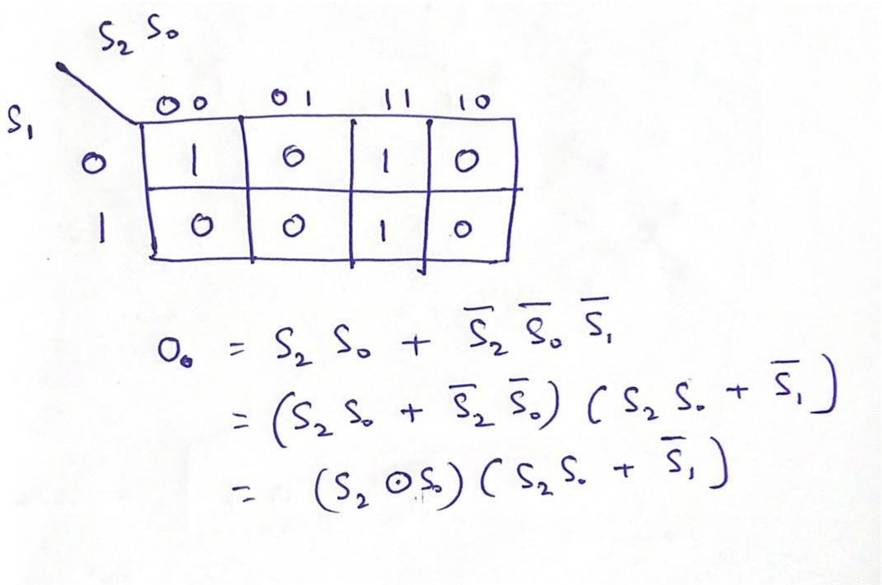


XNOR is used.

S box 2:

K-map for O_0:

The mathematical juggling is done to minimize the number of gates.



S_1 \ $S_2 S_0$	00	01	11	10
0	1	0	1	0
1	0	0	1	0

$$O_0 = S_2 S_0 + \overline{S_2}\,\overline{S_0}\,\overline{S_1}$$

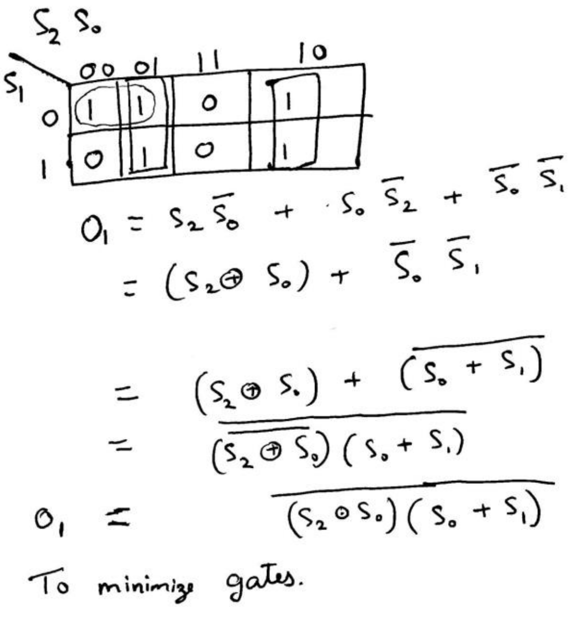
$$= (S_2 S_0 + \overline{S_2}\,\overline{S_0})(S_2 S_0 + \overline{S_1})$$

$$= (S_2 \odot S_0)(S_2 S_0 + \overline{S_1})$$

S box 2:

K-map for O_1:

The mathematical juggling is done to minimize the number of gates.



S_1 \ $S_2 S_0$	00	01	11	10
0	1	1	0	1
1	0	1	0	1

$$O_1 = S_2 \overline{S_0} + S_0 \overline{S_2} + \overline{S_0}\,\overline{S_1}$$

$$= (S_2 \oplus S_0) + \overline{S_0}\,\overline{S_1}$$

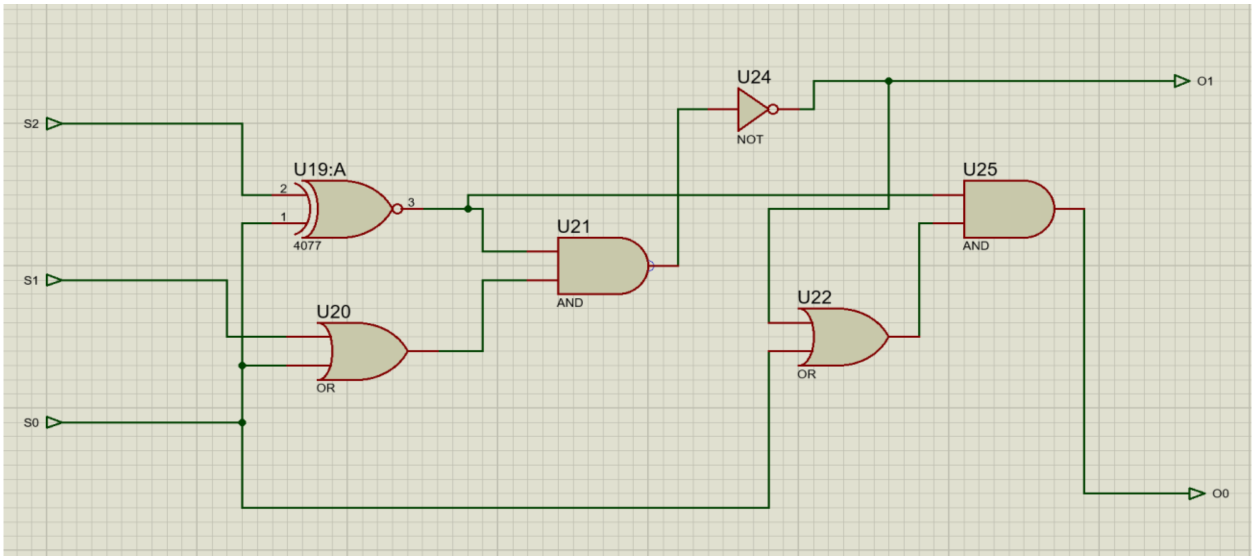
$$= (S_2 \oplus S_0) + \overline{(S_0 + S_1)}$$

$$= \overline{\overline{(S_2 \oplus S_0)}(S_0 + S_1)}$$

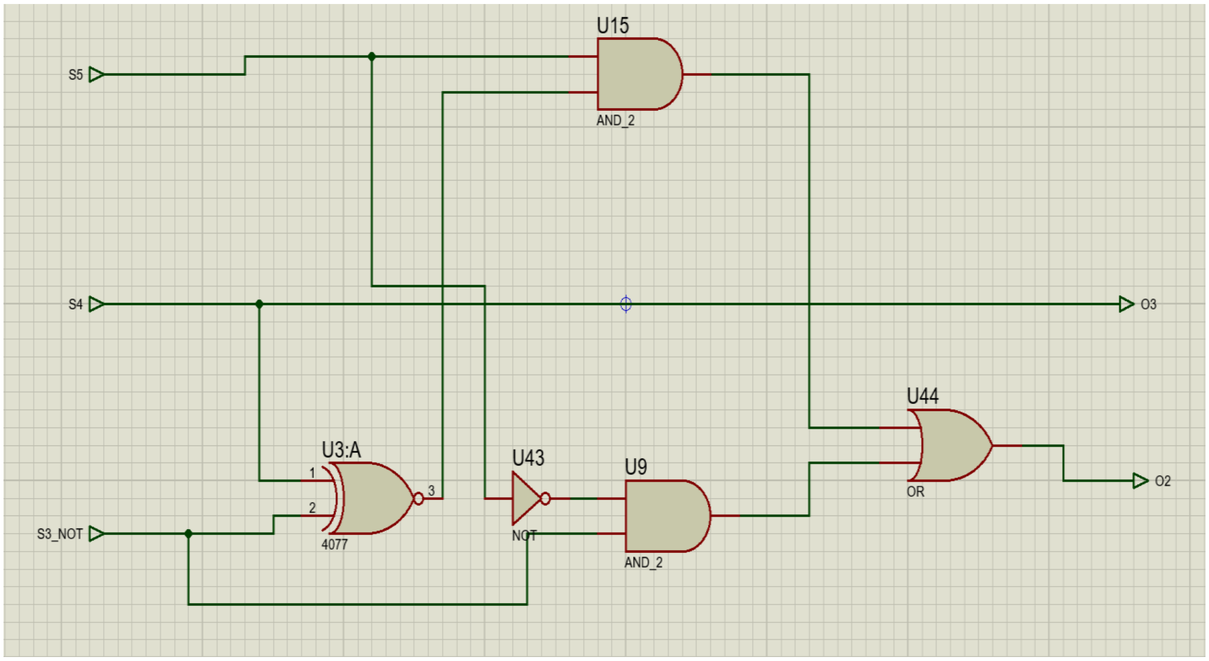
$$O_1 = \overline{(S_2 \odot S_0)(S_0 + S_1)}$$

To minimize gates.

Implementation of S-box 2



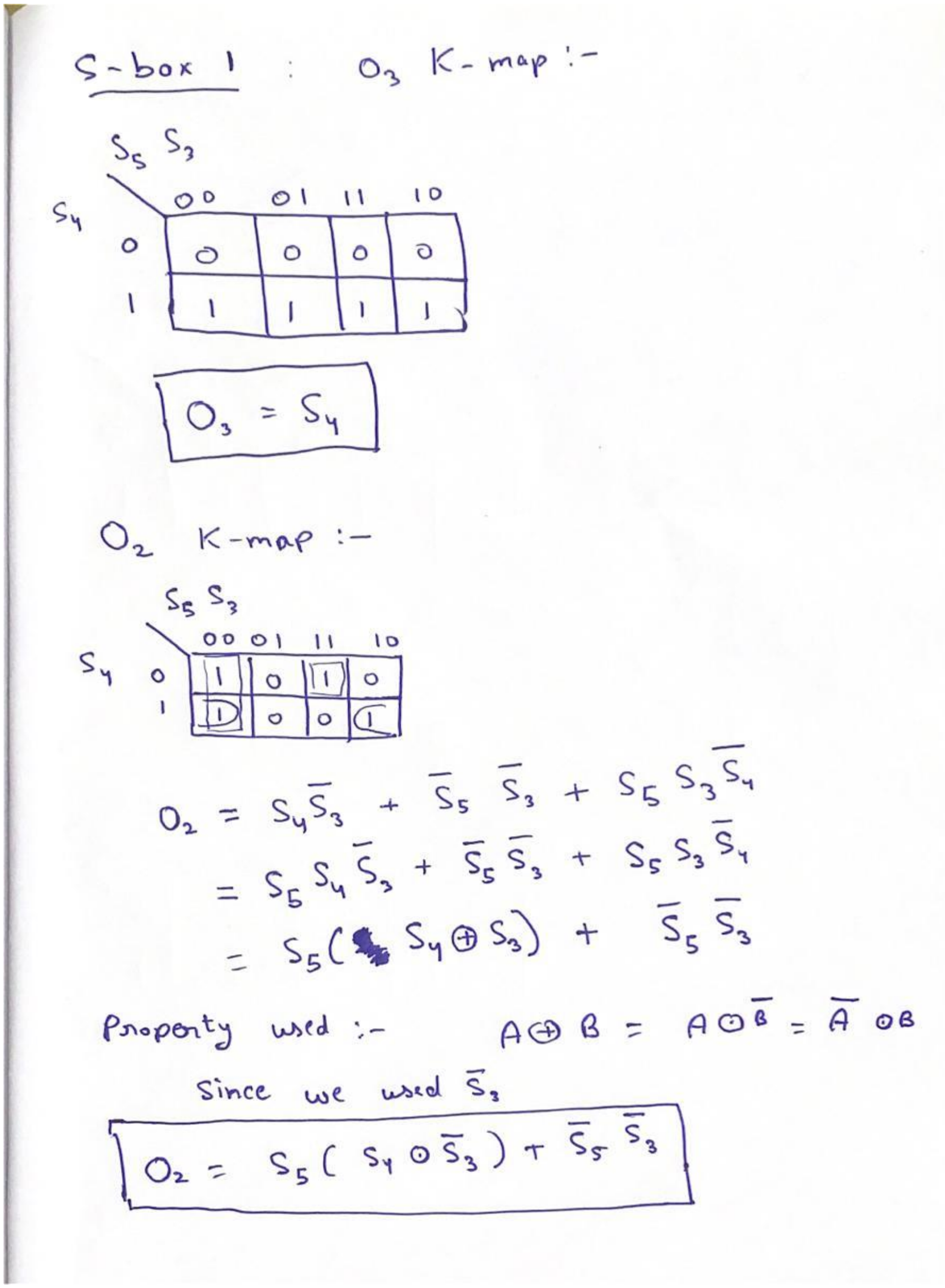
Implementation of S-box 1



S-box 1:

K-map for O_3 and O_2:

From equation of O_2, we see that only S3_NOT is needed.



S-box 1 : O_3 K-map :-

S_4 \ $S_5 S_3$	00	01	11	10
0	0	0	0	0
1	1	1	1	1

$$\boxed{O_3 = S_4}$$

O_2 K-map :-

S_4 \ $S_5 S_3$	00	01	11	10
0	1	0	1	0
1	1	0	0	1

$$O_2 = S_4\bar{S}_3 + \bar{S}_5\bar{S}_3 + S_5 S_3 \bar{S}_4$$
$$= S_5 S_4 \bar{S}_3 + \bar{S}_5\bar{S}_3 + S_5 S_3 \bar{S}_4$$
$$= S_5(S_4 \oplus S_3) + \bar{S}_5\bar{S}_3$$

Property used :- $A \oplus B = A \odot \bar{B} = \bar{A} \odot B$

Since we used $\bar{S}_3$

$$\boxed{O_2 = S_5(S_4 \odot \bar{S}_3) + \bar{S}_5\bar{S}_3}$$