

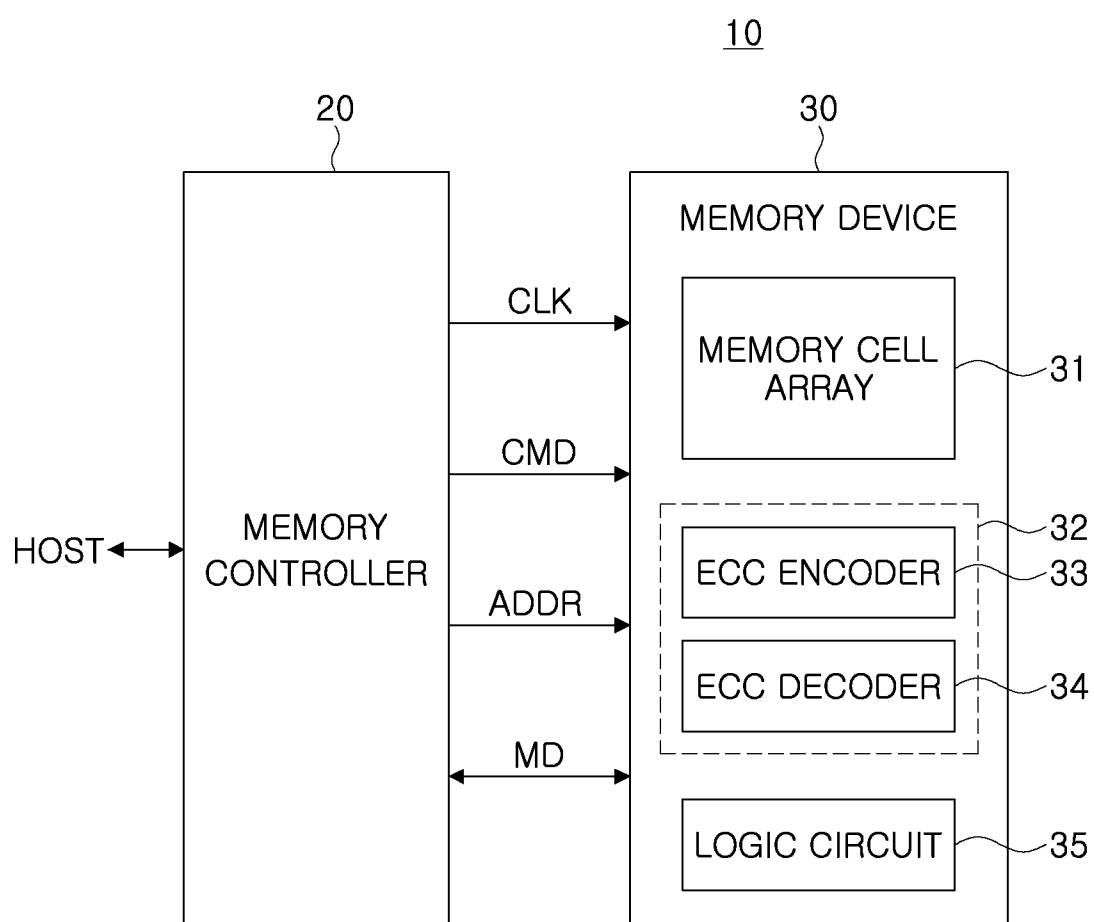


FIG. 1

K0	K1	K2	K3	P0	P1	P2	P3
1	1	1	0	1	0	0	0
1	1	0	1	0	1	0	0
1	0	1	1	0	0	1	0
0	1	1	1	0	0	0	1

$$P0 = K0 \oplus K1 \oplus K2$$

$$P1 = K0 \oplus K1 \oplus K3$$

$$P2 = K0 \oplus K2 \oplus K3$$

$$P3 = K1 \oplus K2 \oplus K3$$

FIG. 2

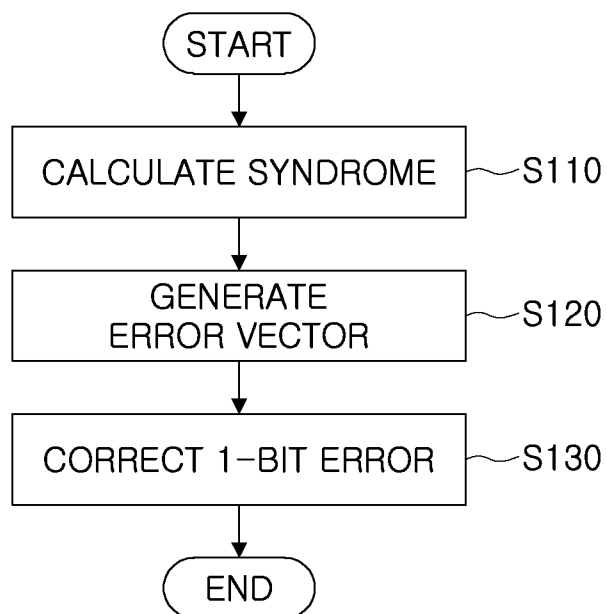
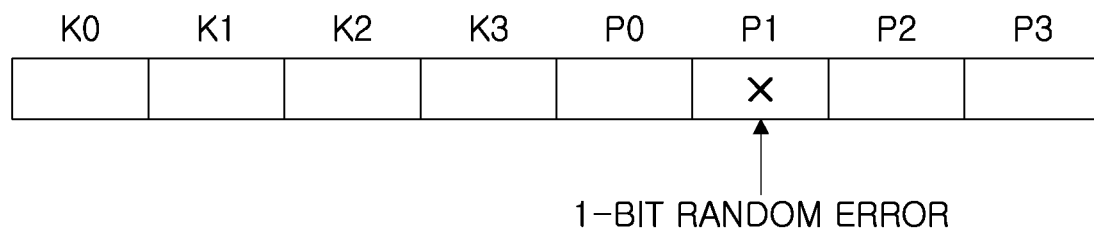


FIG. 3



$$S = H \times y$$
$$x = y \oplus v$$

FIG. 4

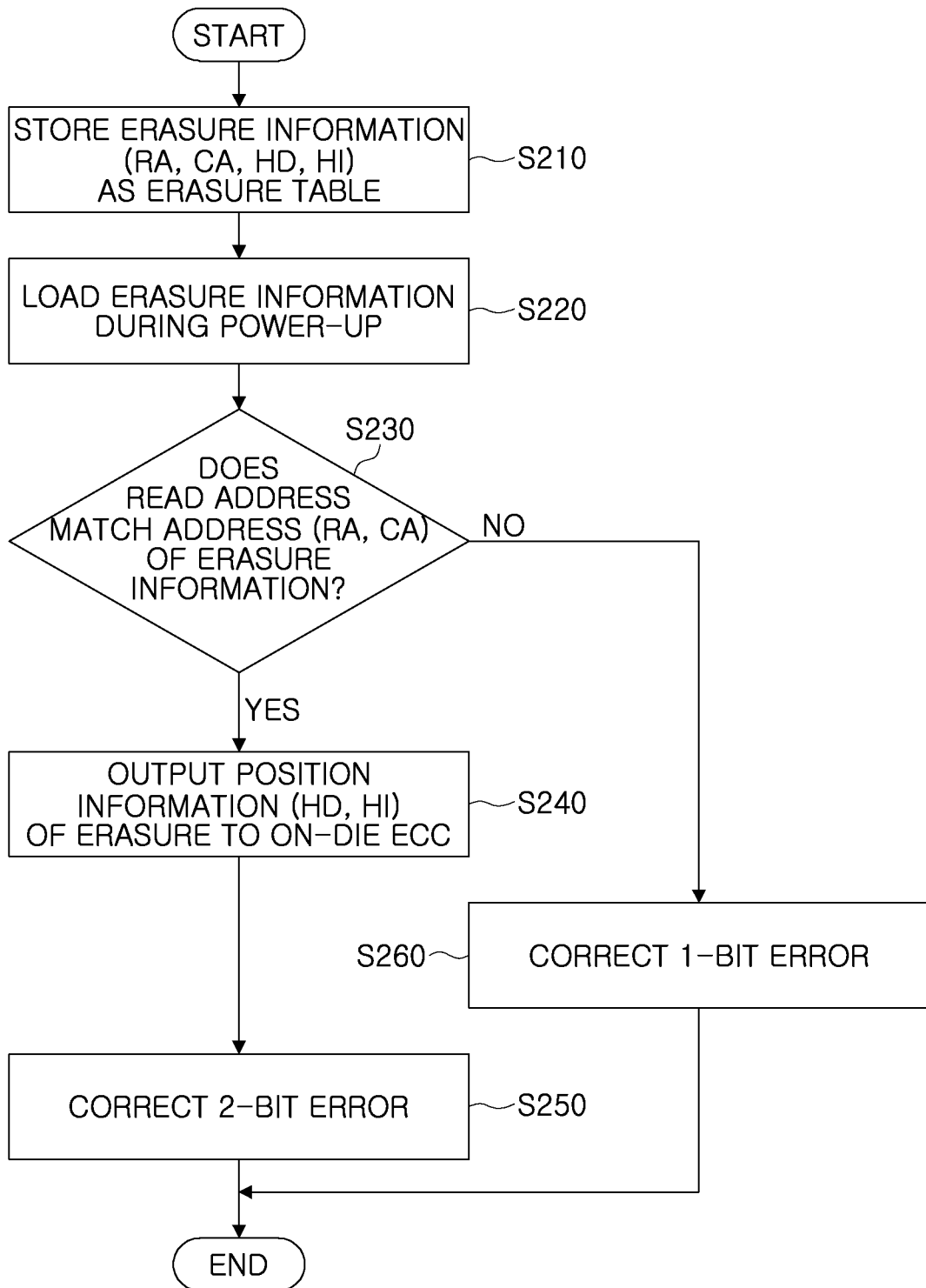


FIG. 5

RA	CA	HD	HI
RA[0]	CA[0]	HD[0]	HI[0]
RA[1]	CA[1]	HD[1]	HI[1]
⋮	⋮	⋮	⋮
RA[n-1]	CA[n-1]	HD[n-1]	HI[n-1]

FIG. 6

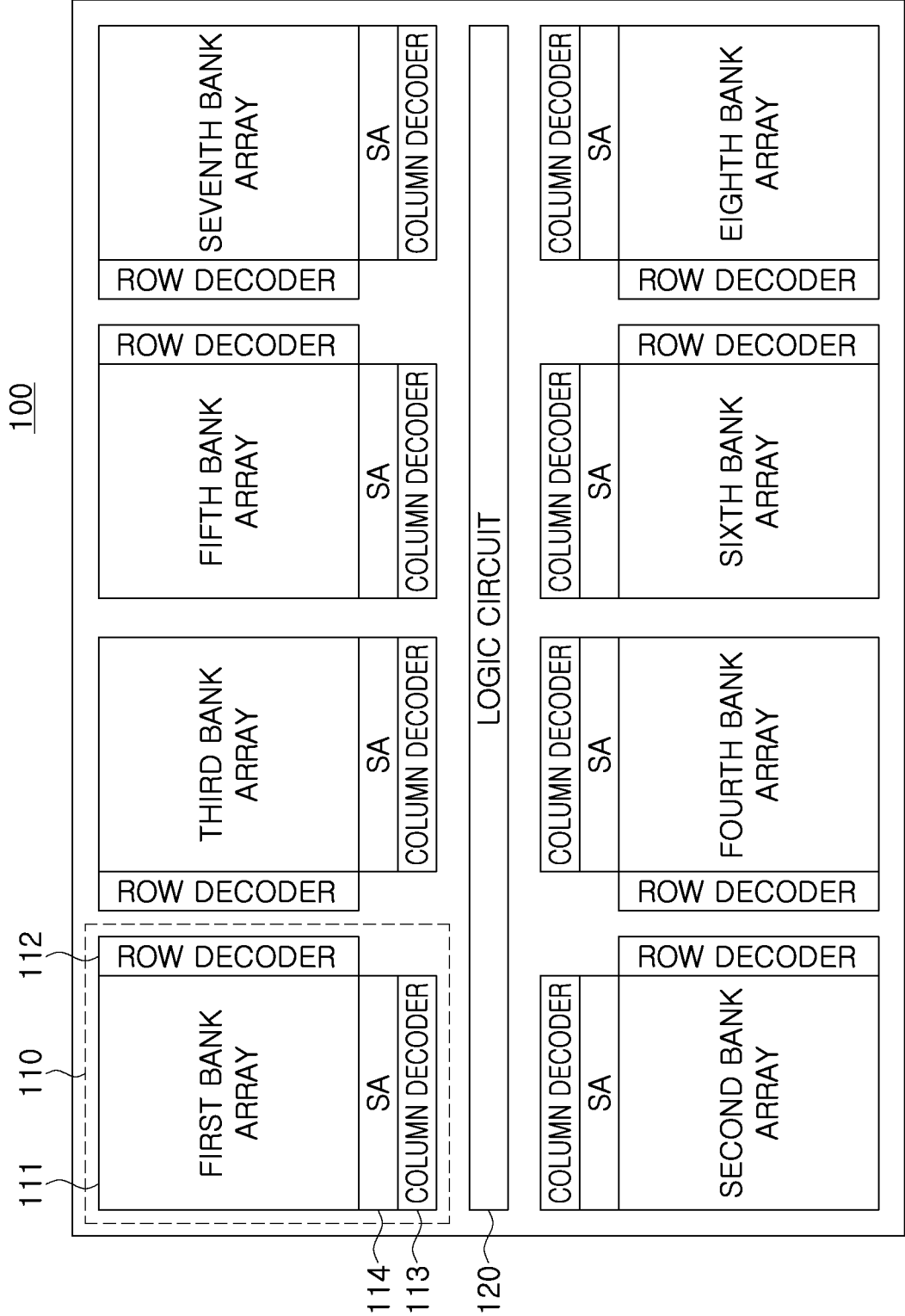


FIG. 7

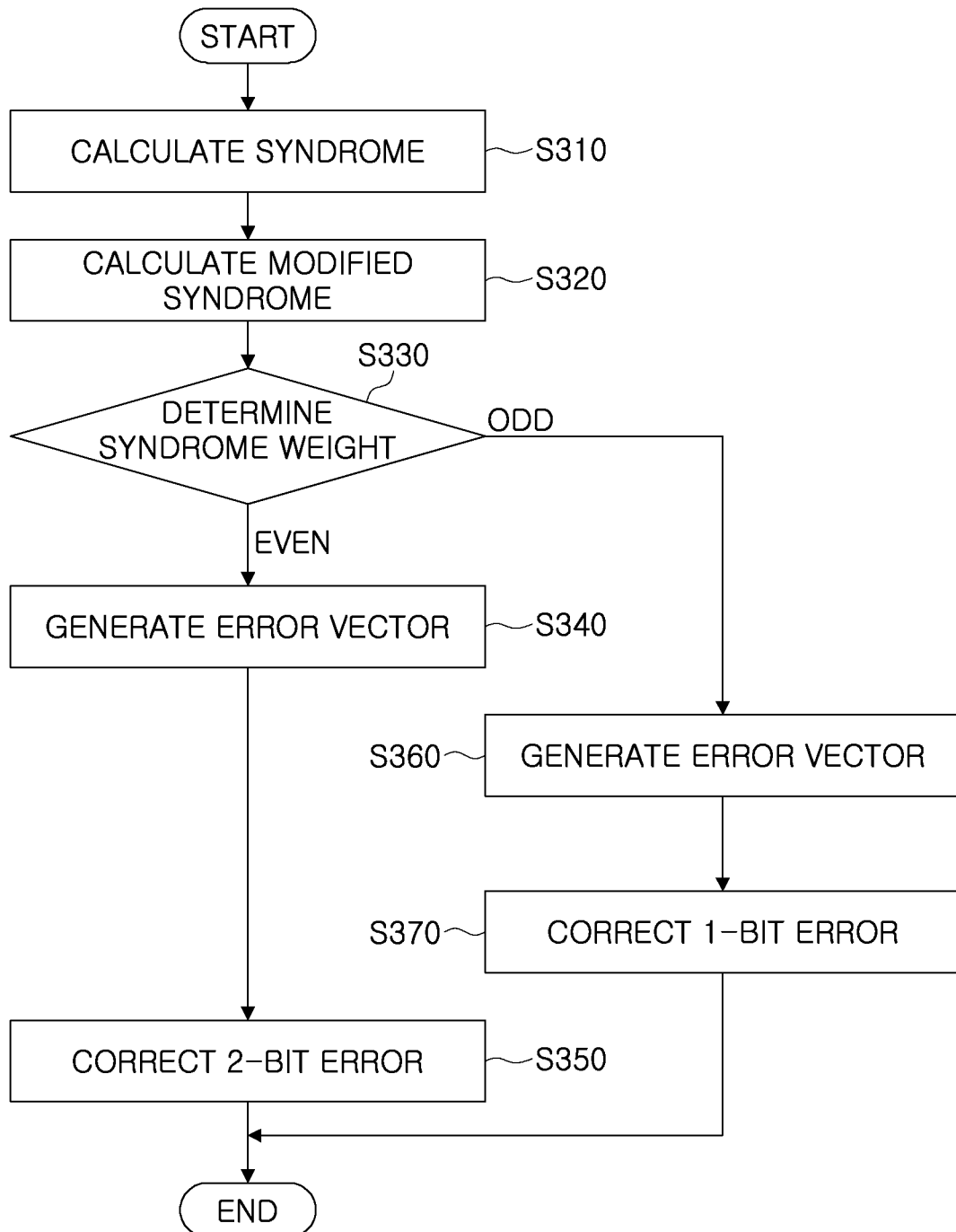
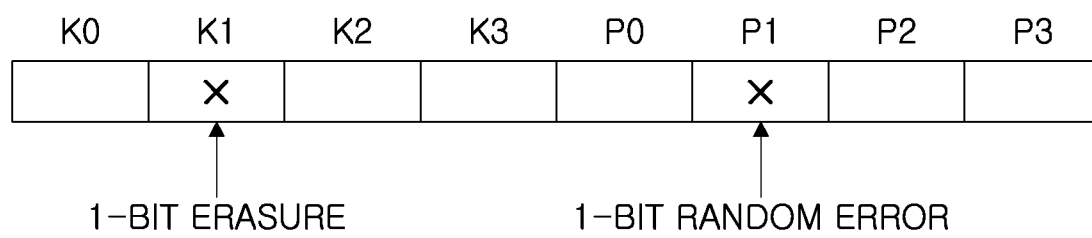


FIG. 8



$$\begin{aligned}S &= H \times y \\MS &= S \oplus HD \\x &= y \oplus v\end{aligned}$$

FIG. 9

200

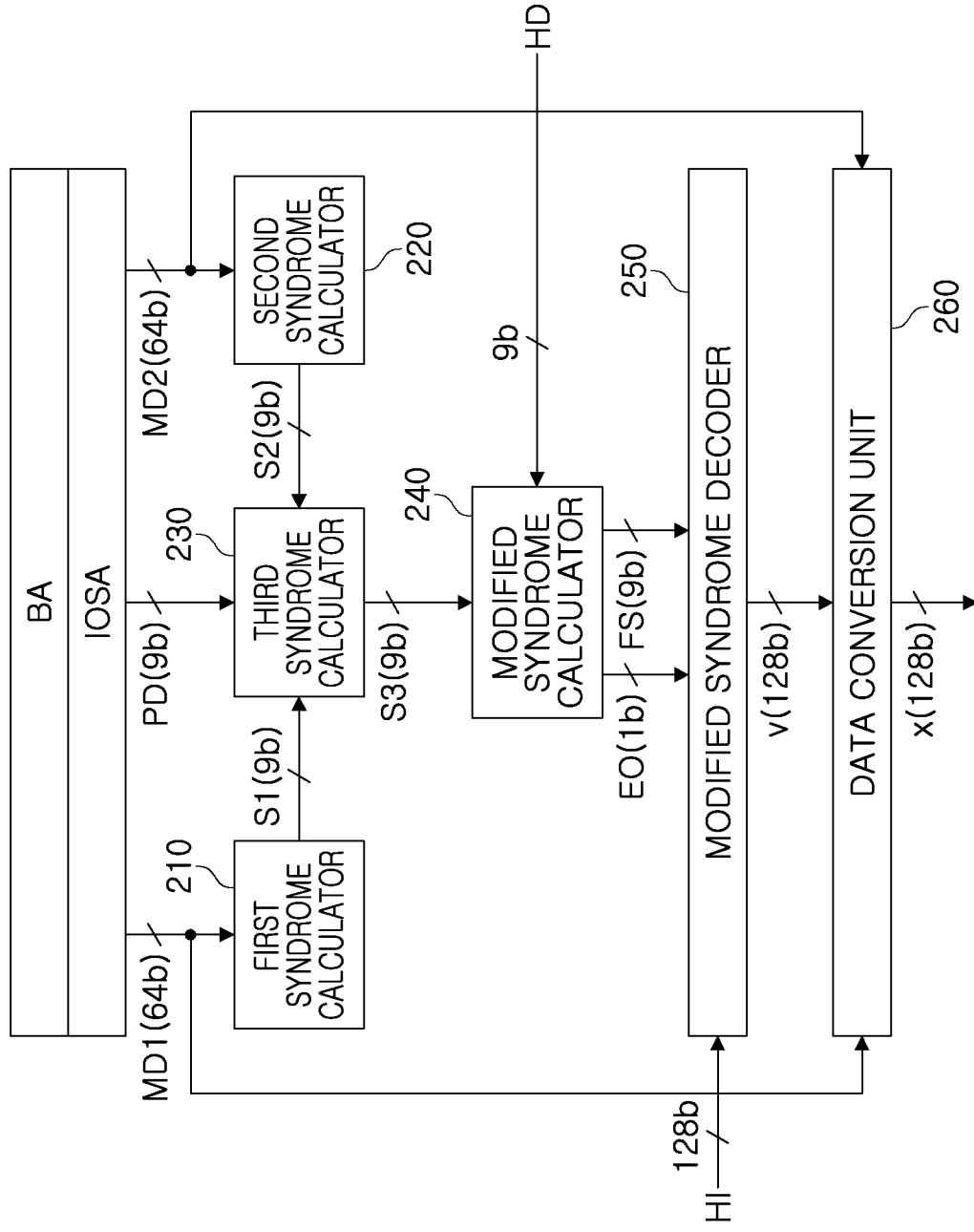


FIG. 10

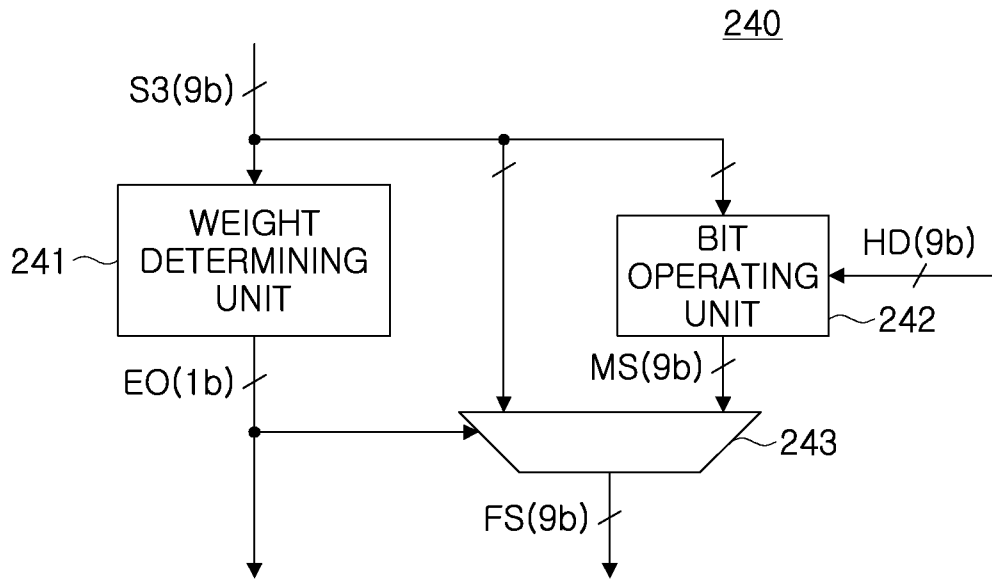


FIG. 11

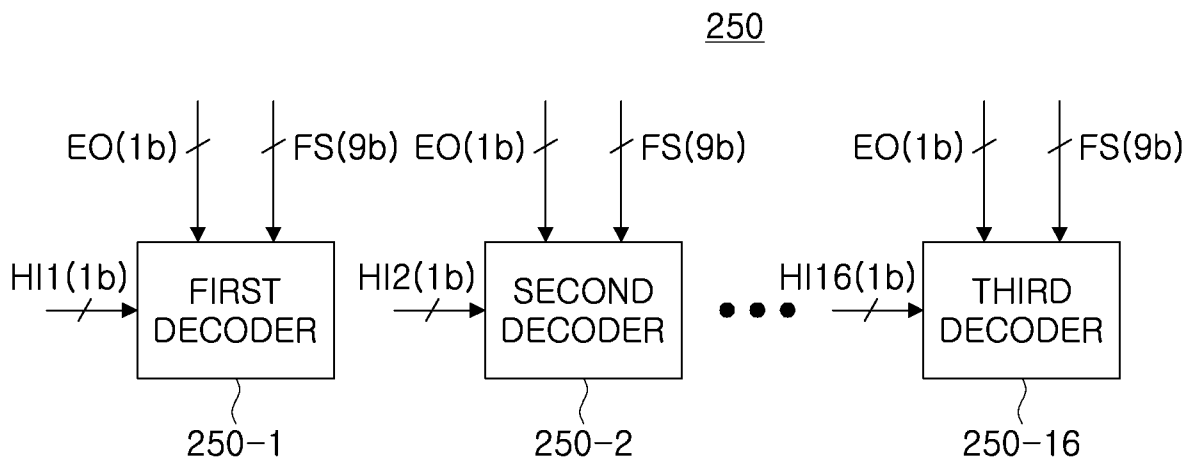


FIG. 12

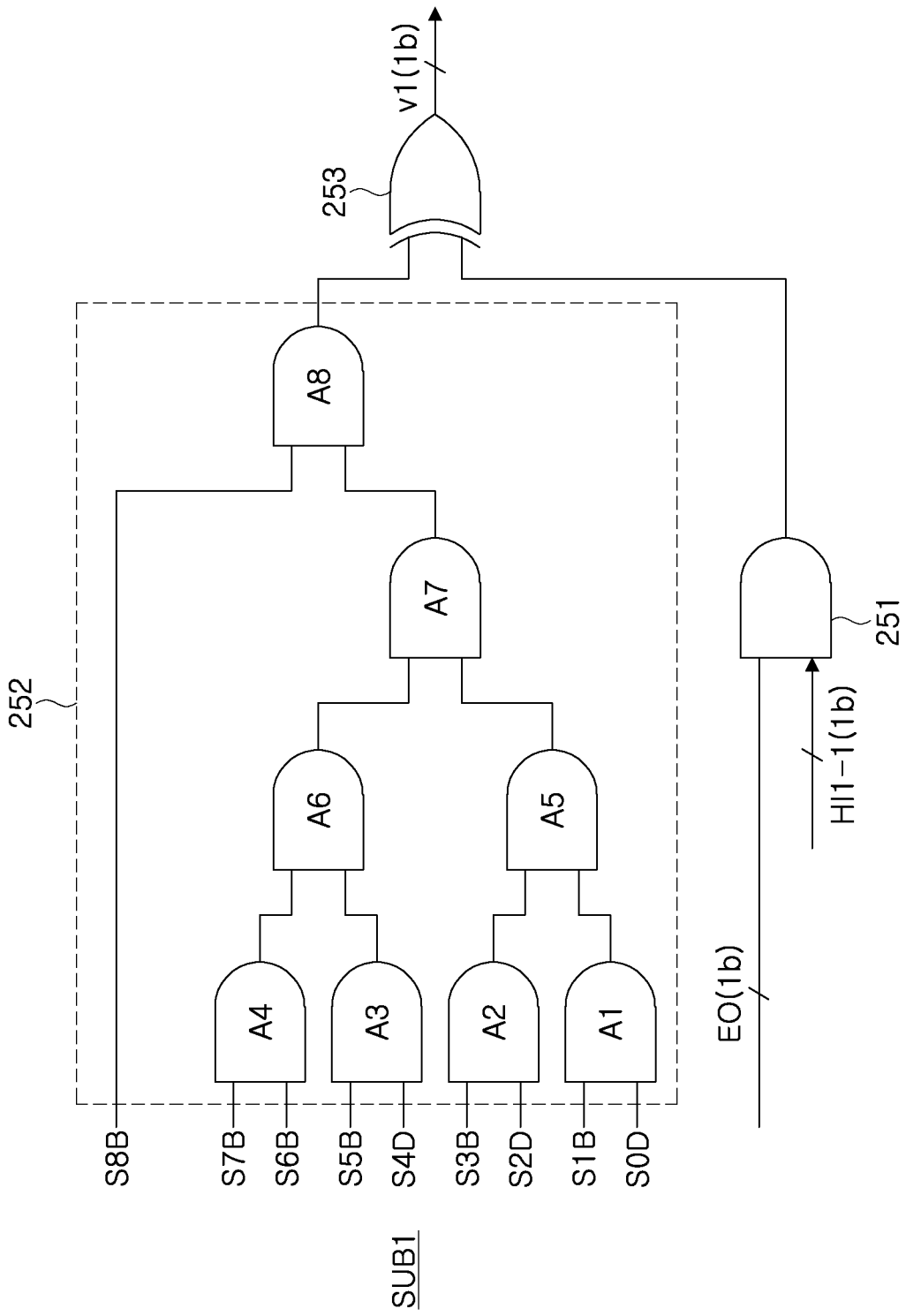


FIG. 13



FIG. 14

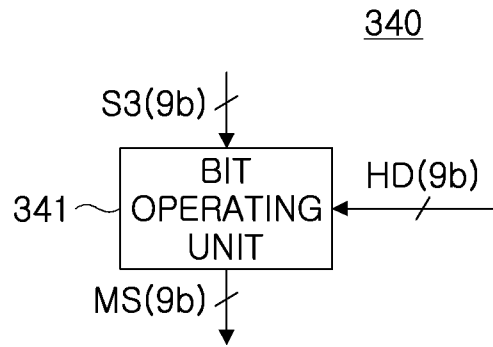


FIG. 15

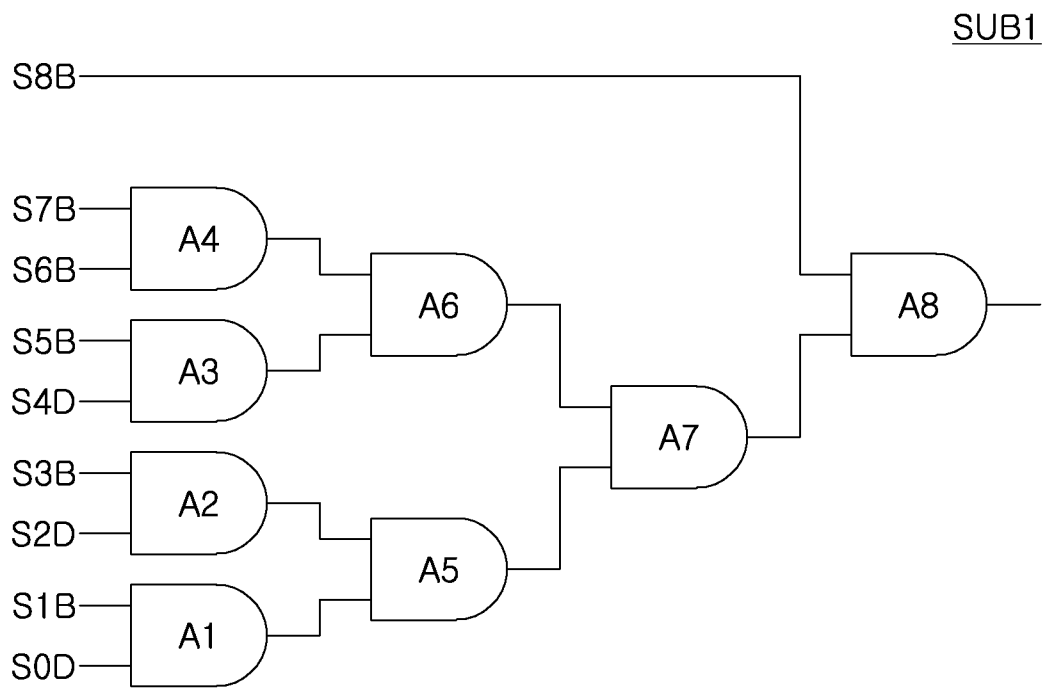


FIG. 16

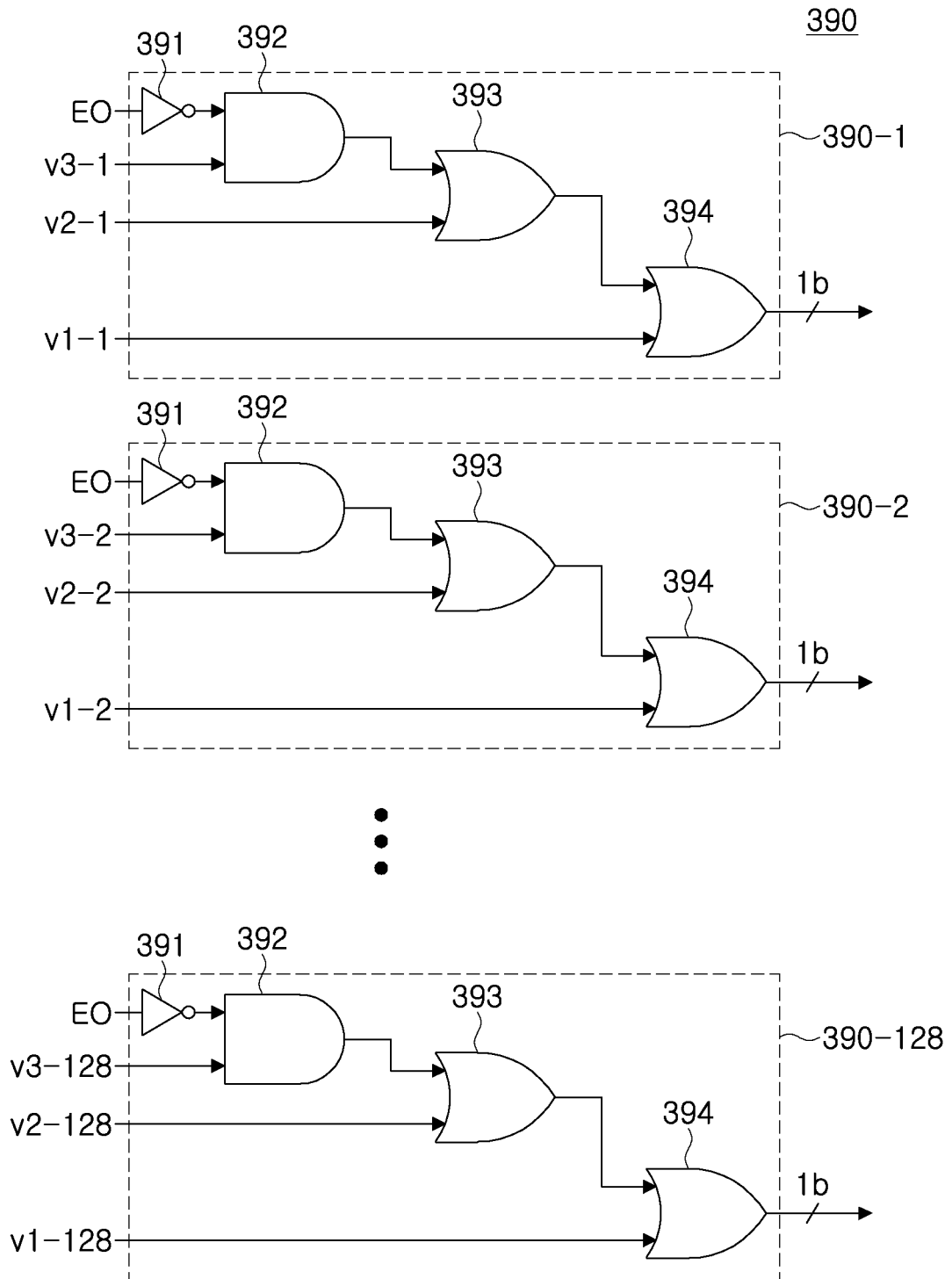


FIG. 17