

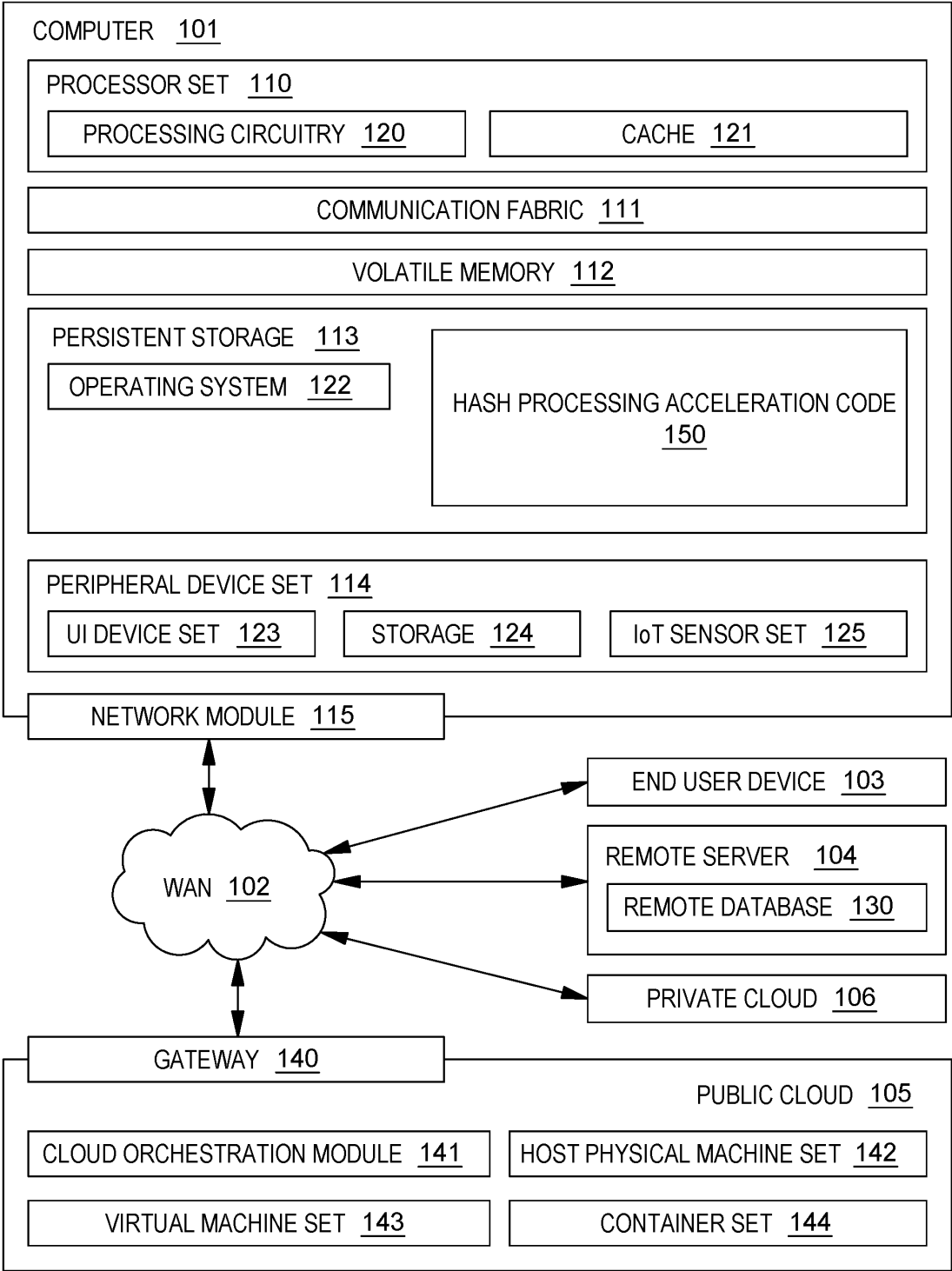


FIG. 1

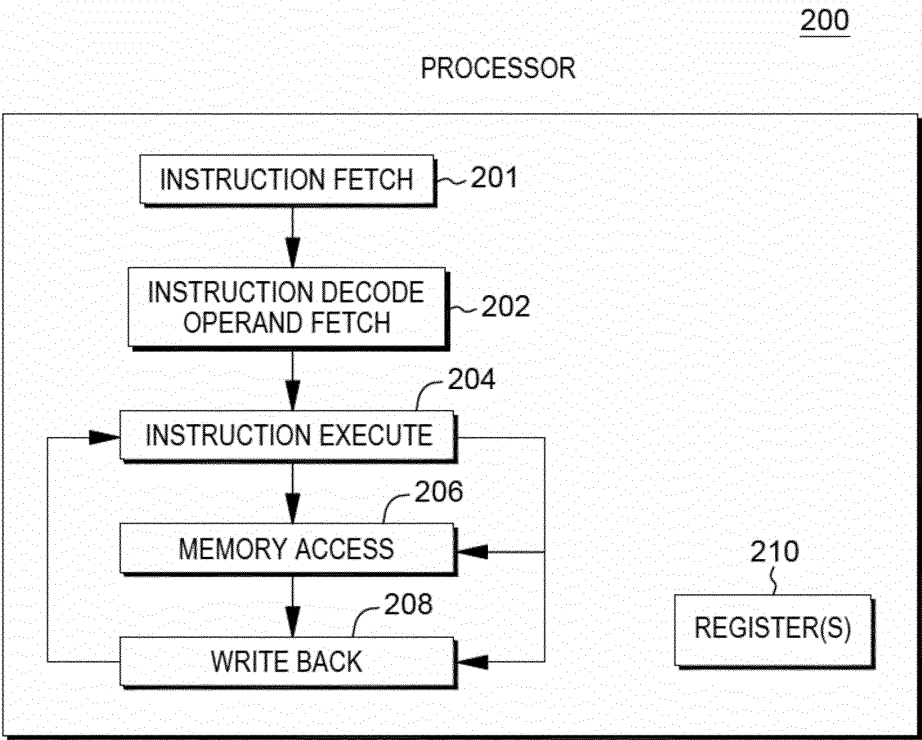


FIG. 2

3/15

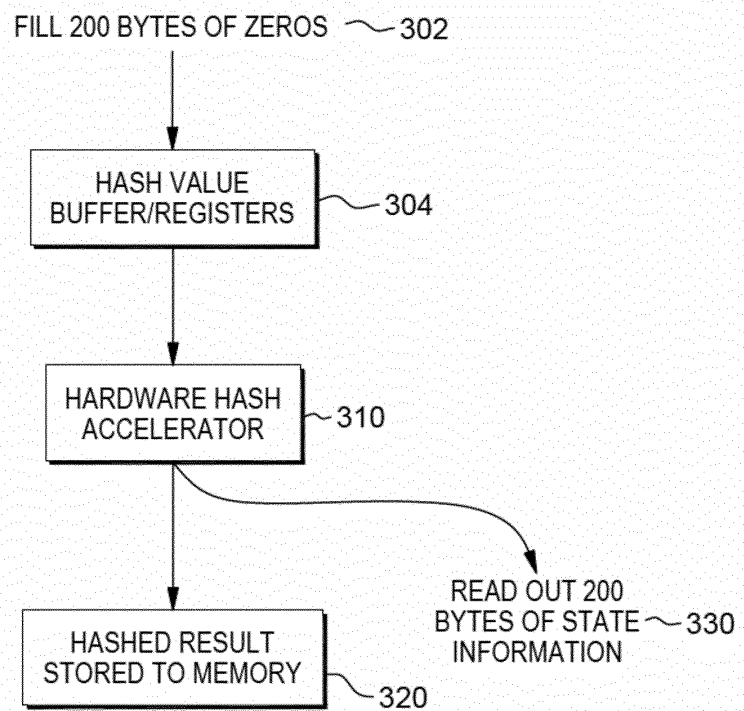


FIG. 3

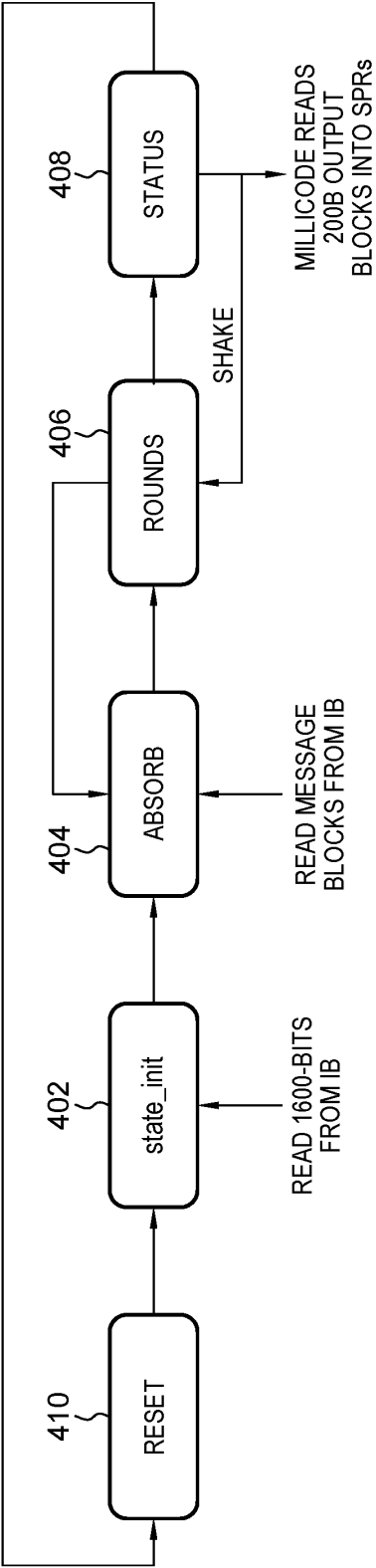


FIG. 4A

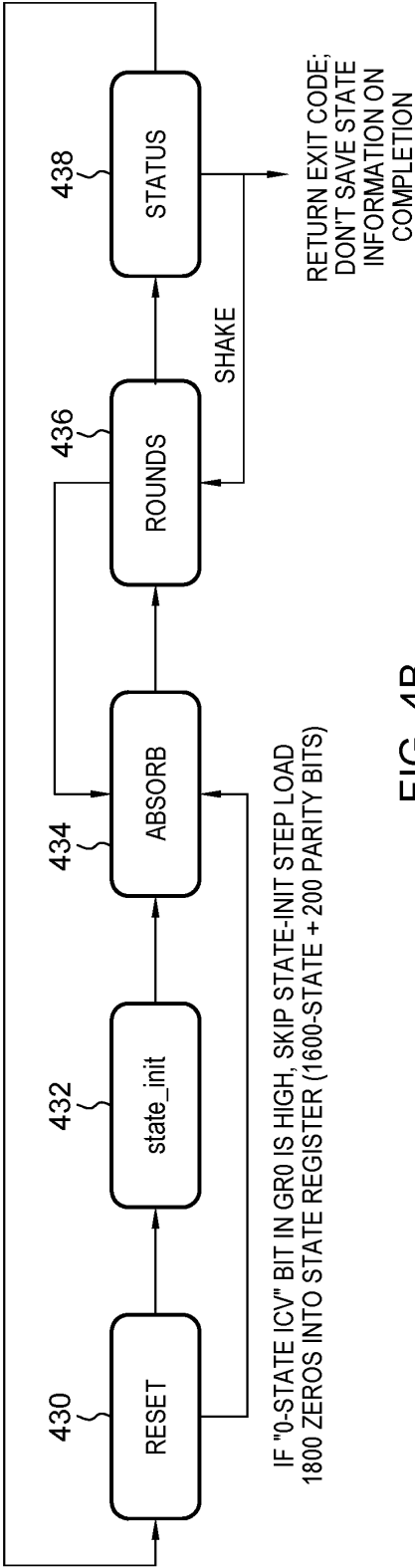


FIG. 4B

5/15

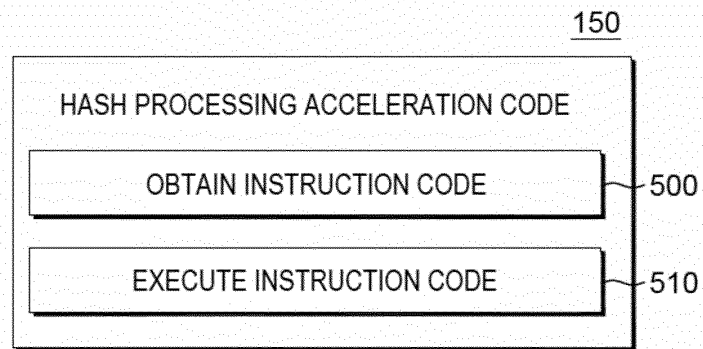


FIG. 5A

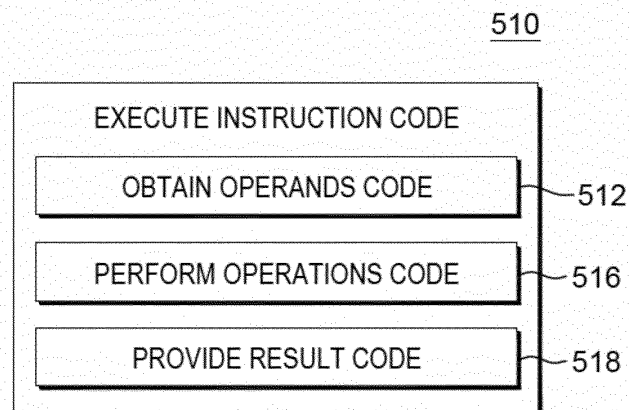


FIG. 5B

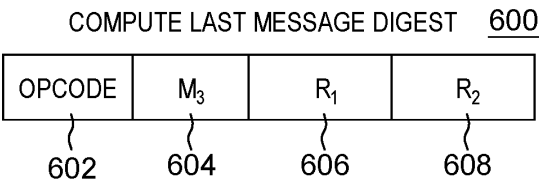


FIG. 6A

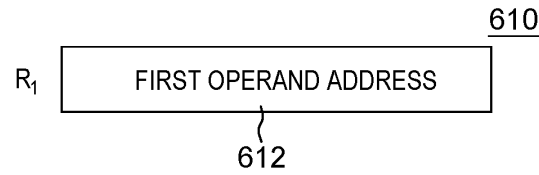


FIG. 6B

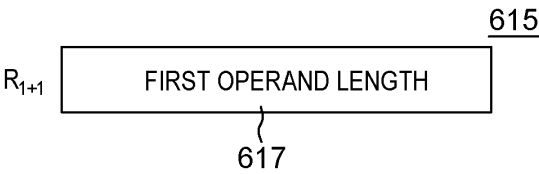


FIG. 6C

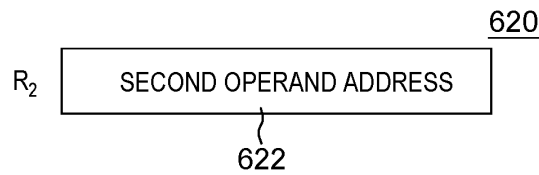


FIG. 6D

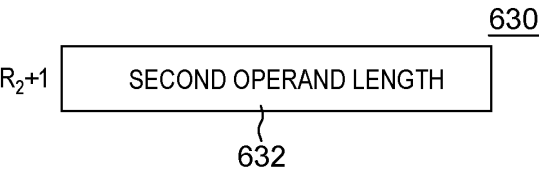


FIG. 6E

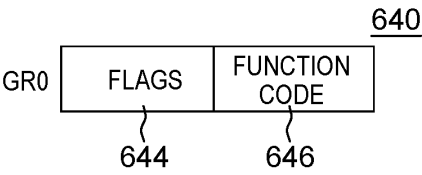


FIG. 6F

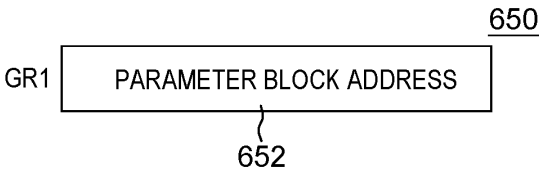


FIG. 6G

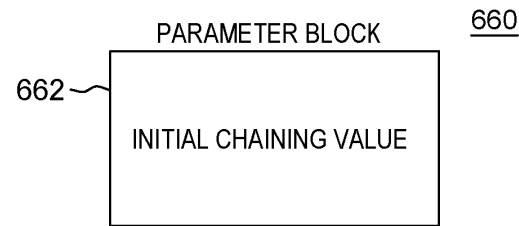


FIG. 6H

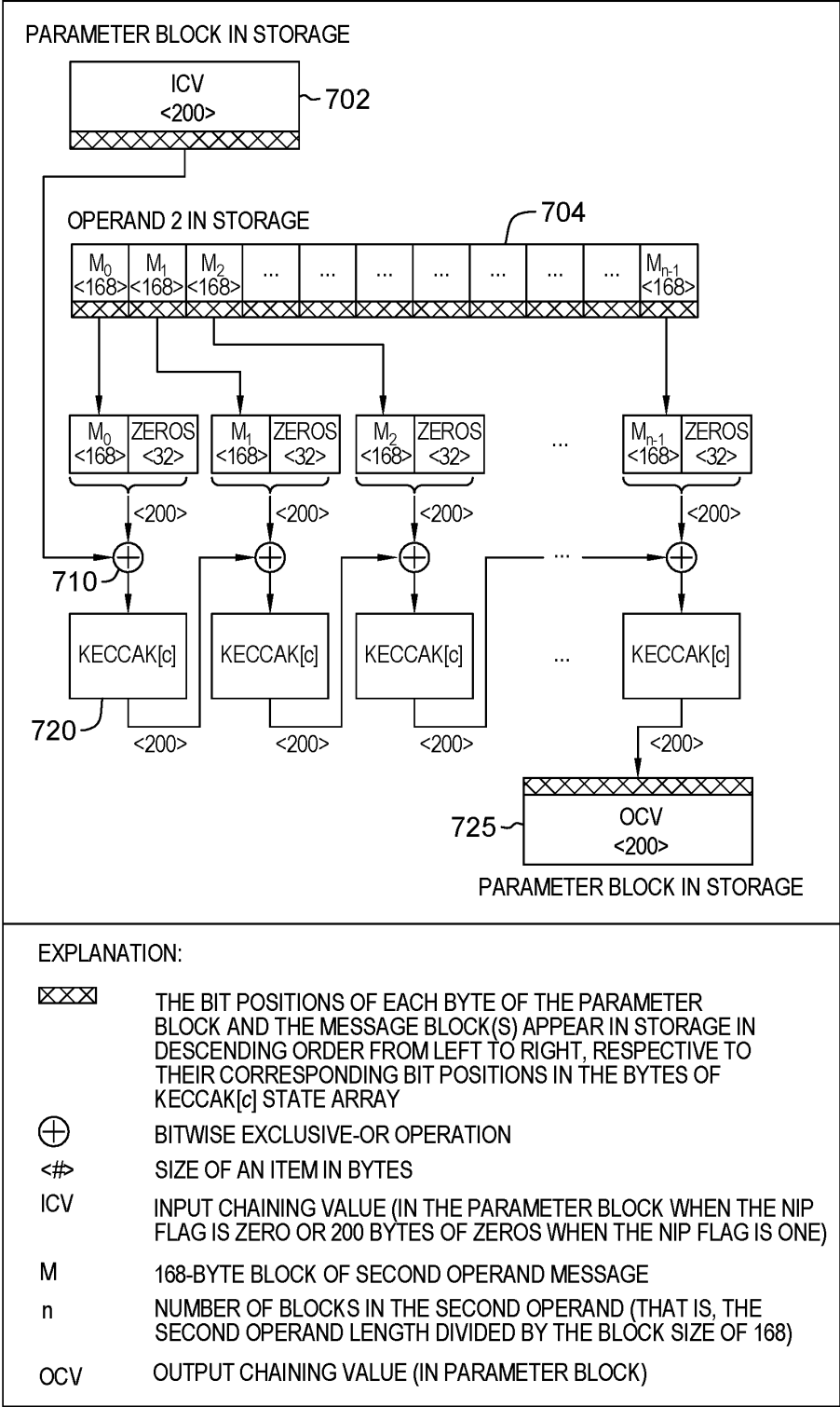
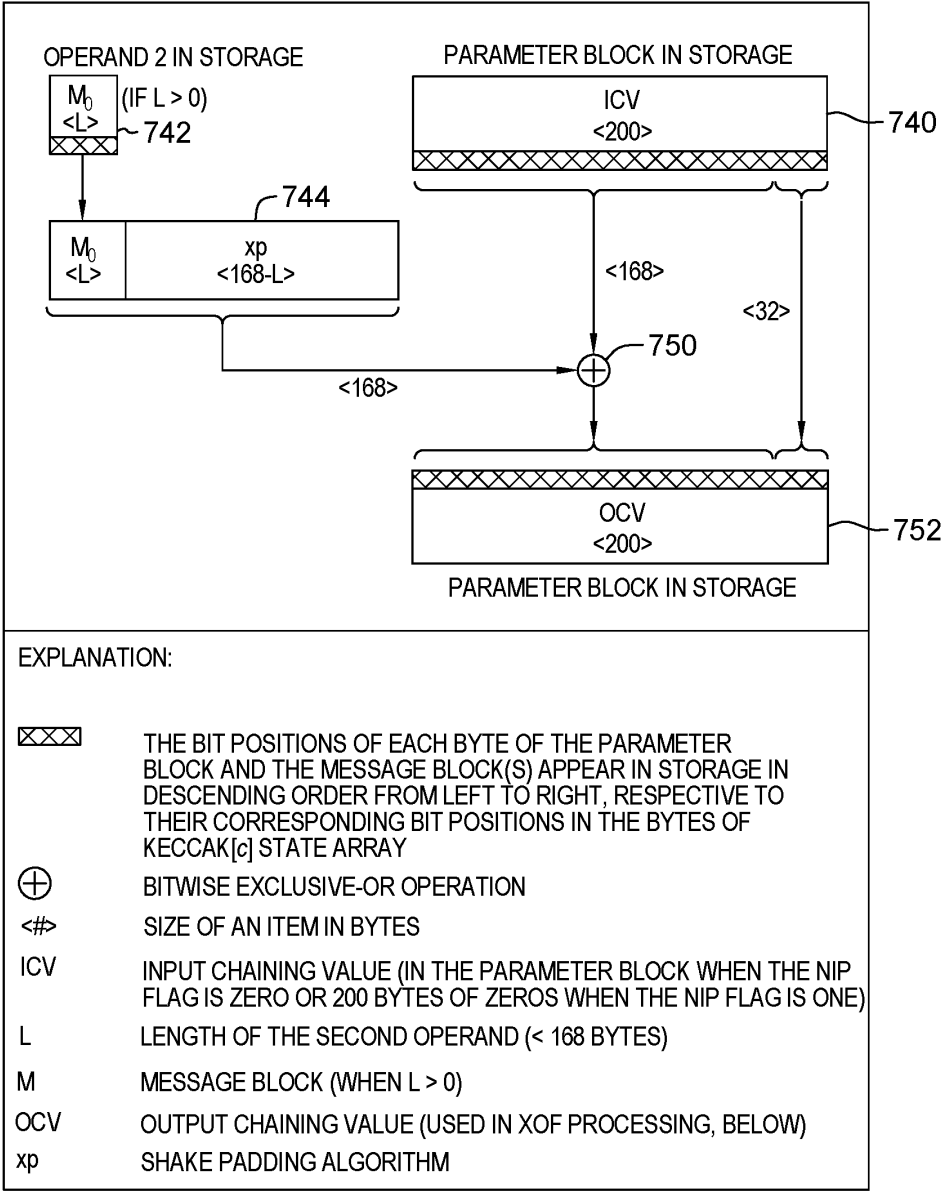


FIG. 7A



KLMD-SHAKE-128 PADDING ($L < 168$)

FIG. 7B

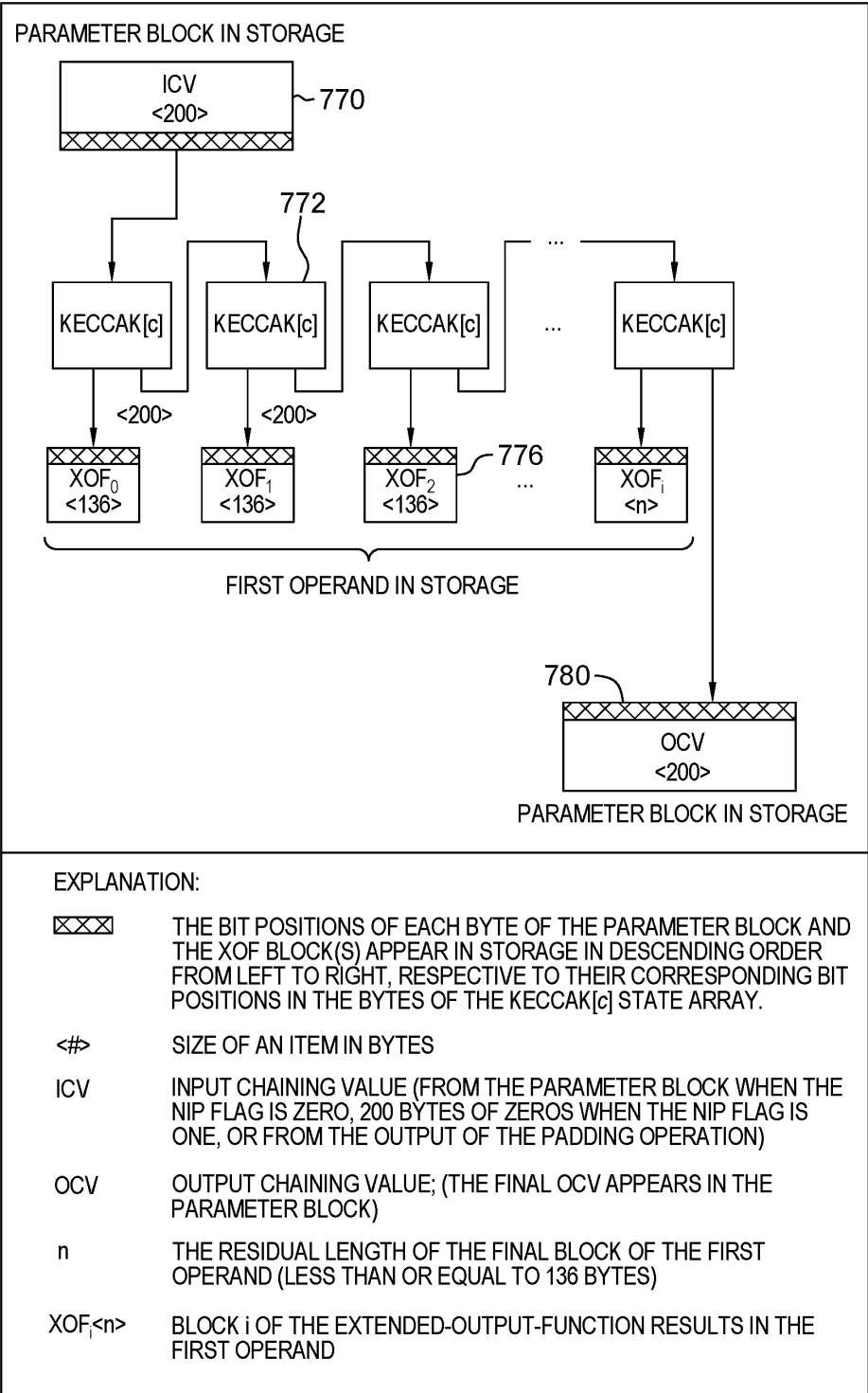


FIG. 7C

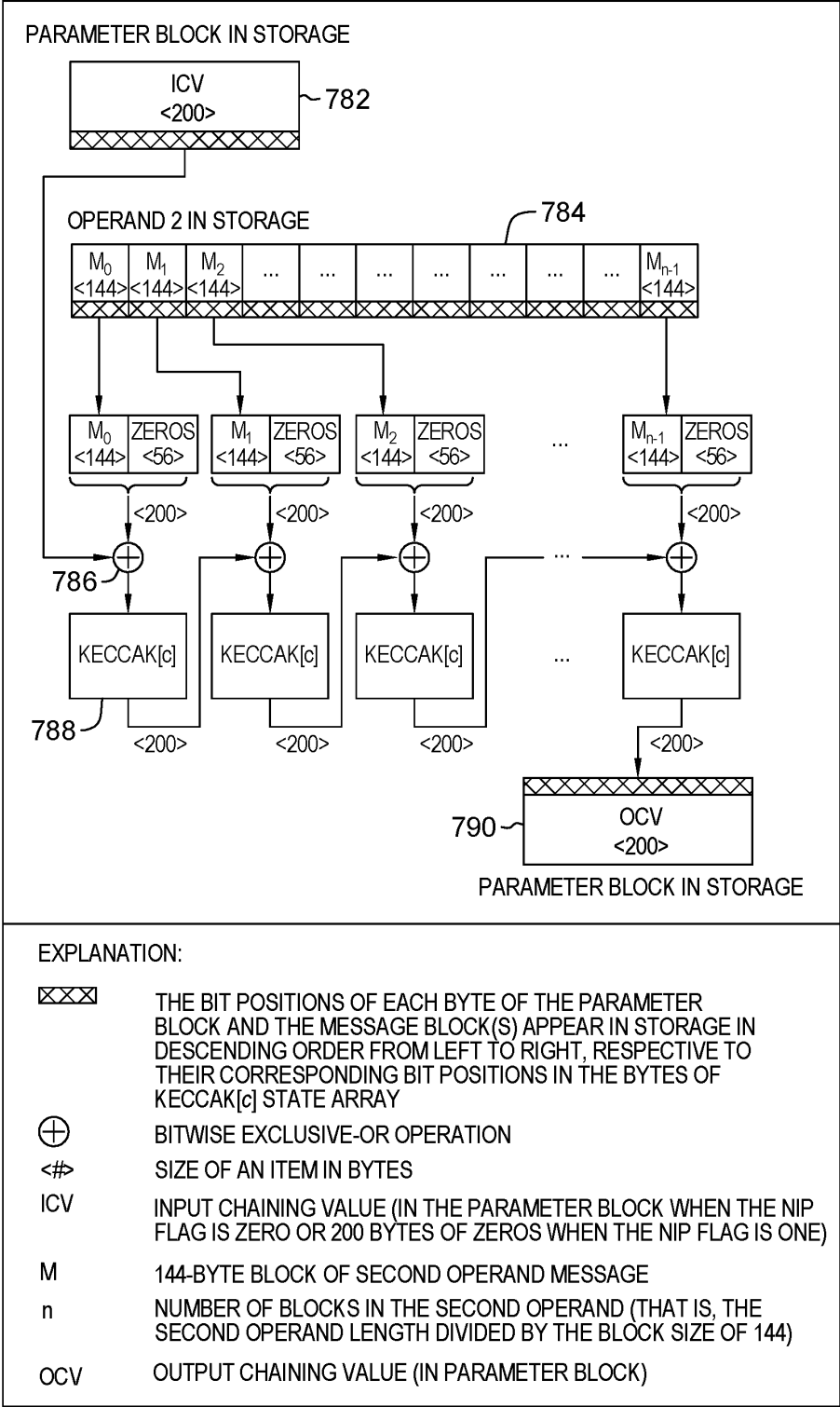
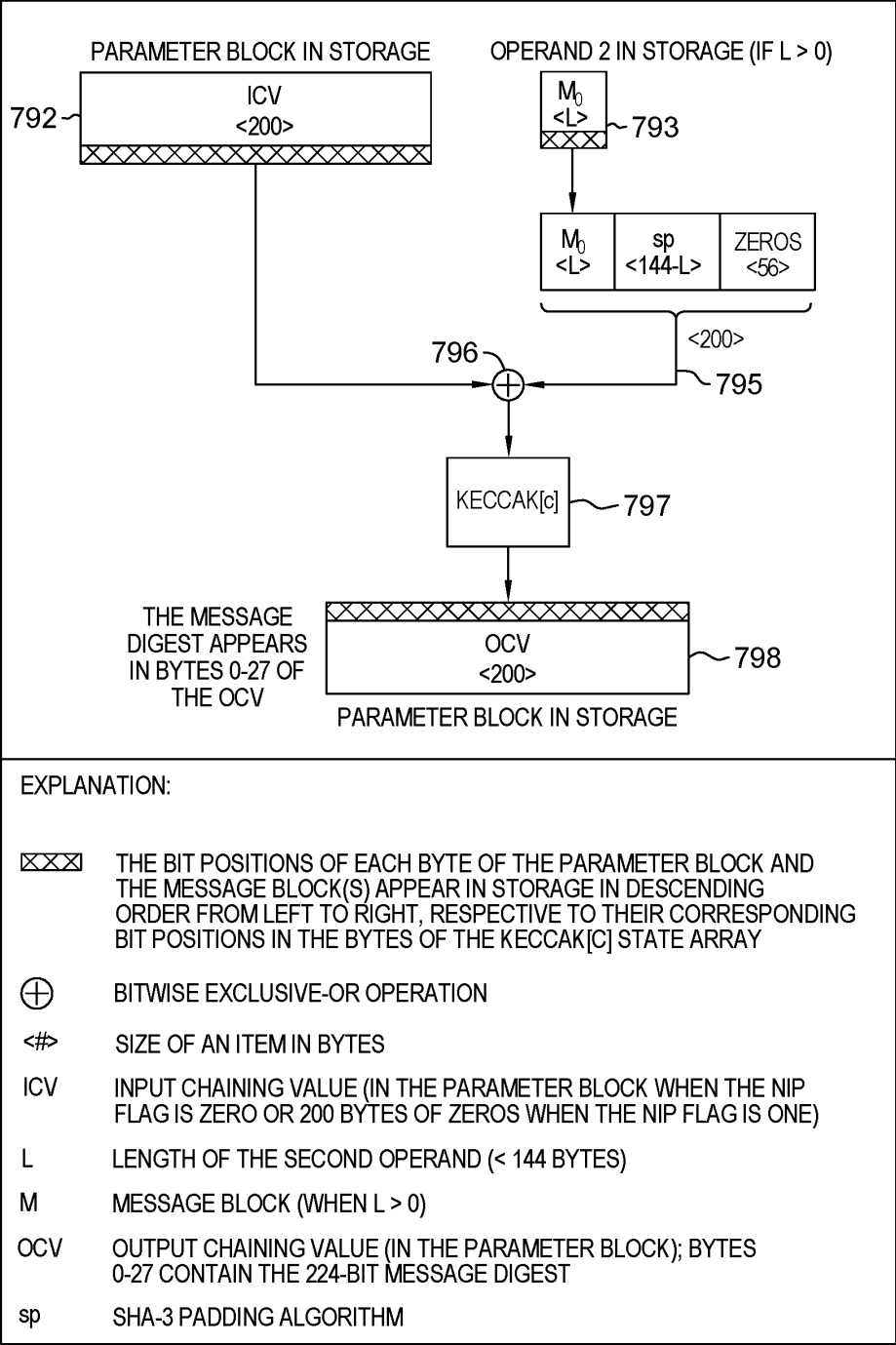


FIG. 7D



KLMD-SHA3-224 PROCESSING (L < 144)

FIG. 7E

12/15

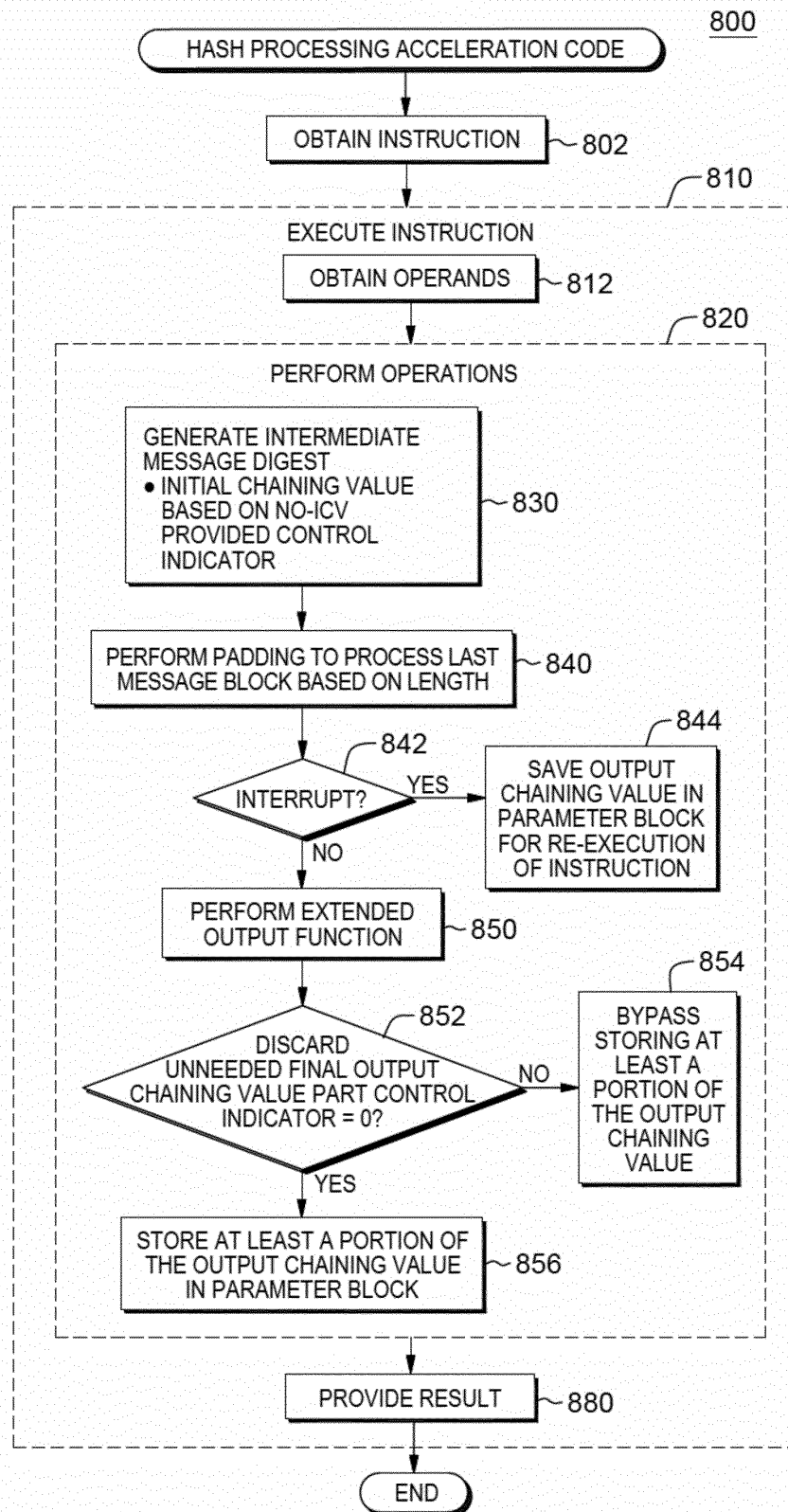


FIG. 8

13/15

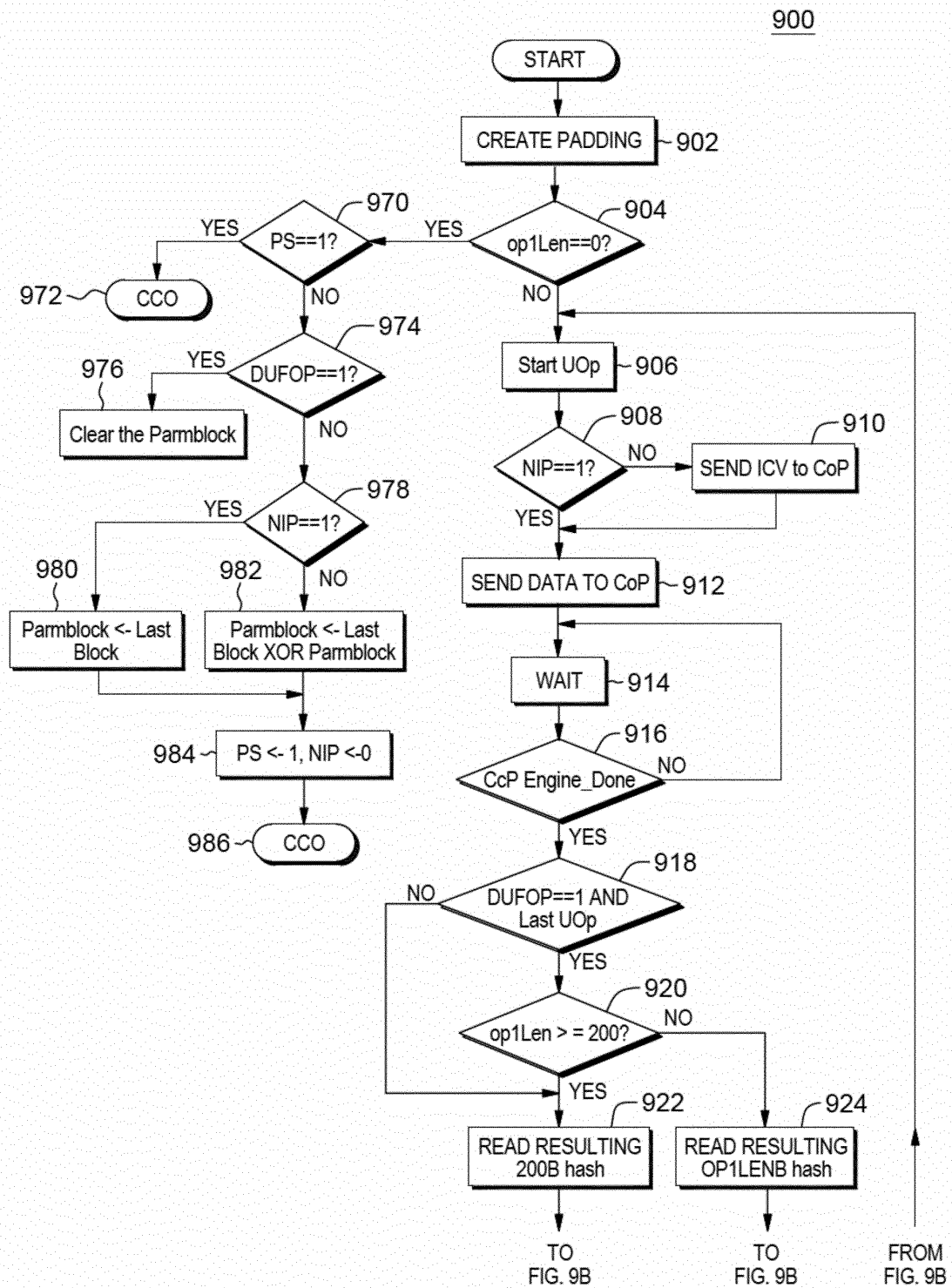


FIG. 9A

14/15

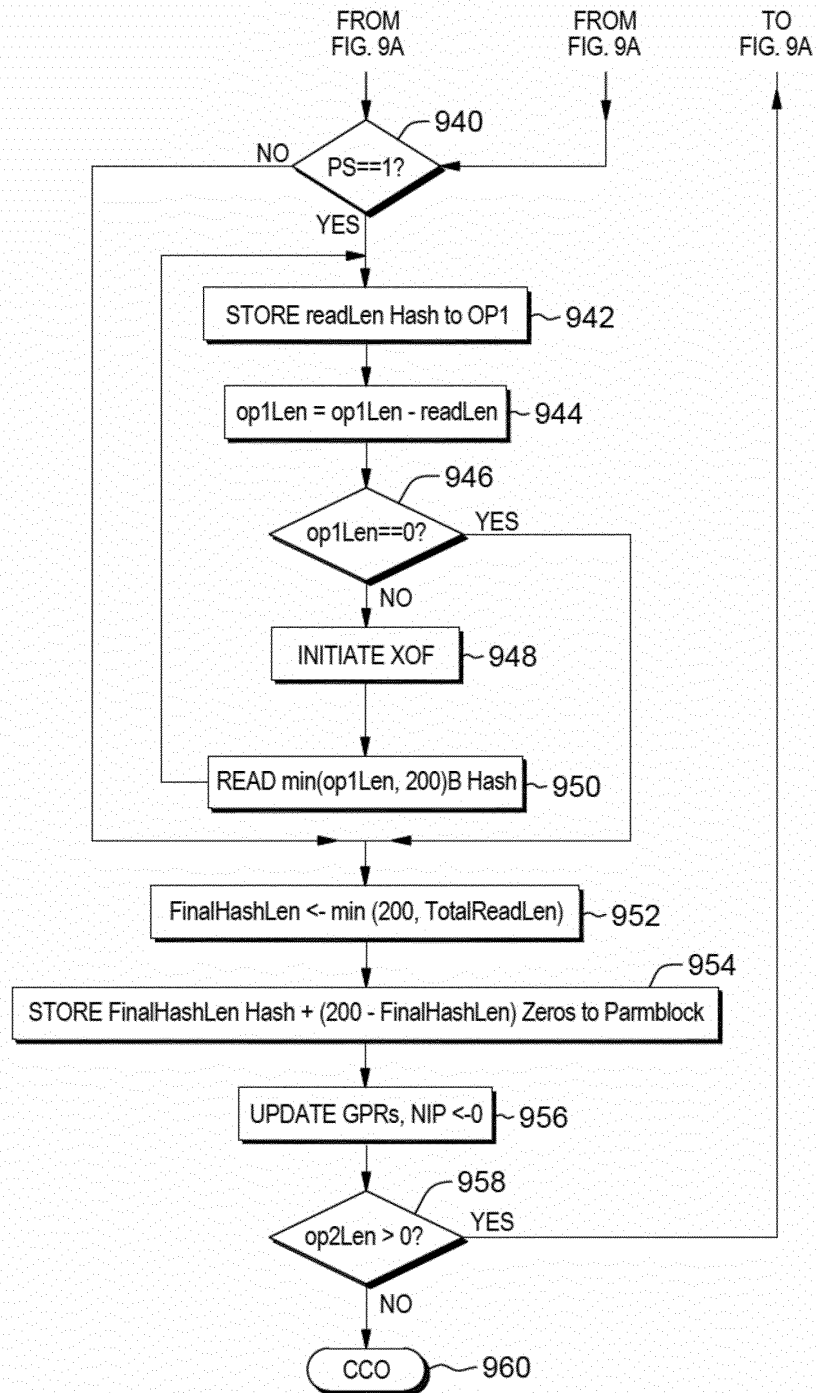


FIG. 9B

15/15

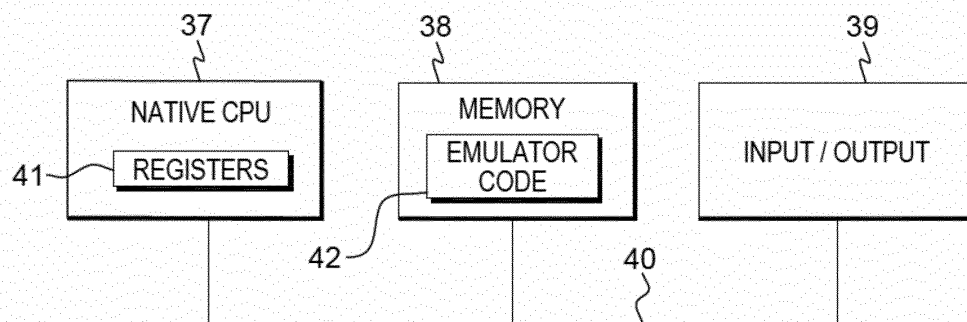
36

FIG. 10A

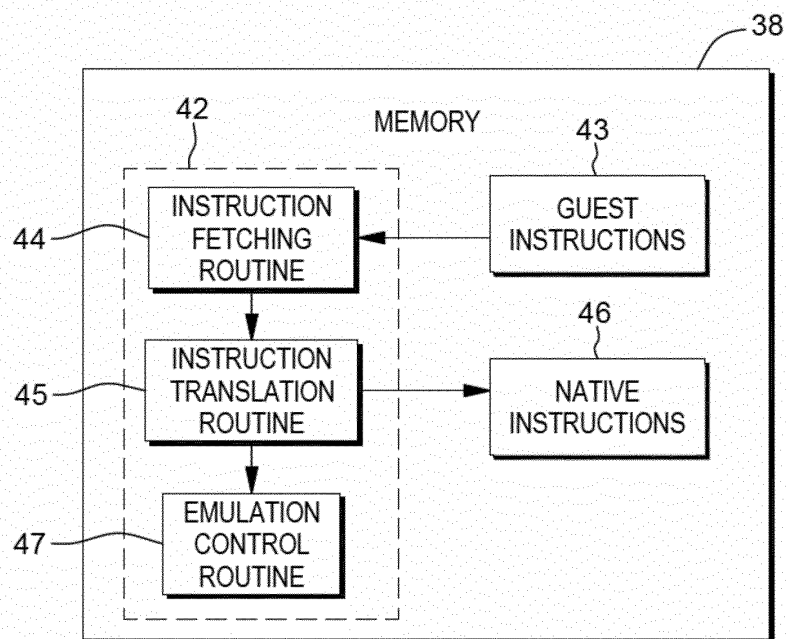


FIG. 10B