

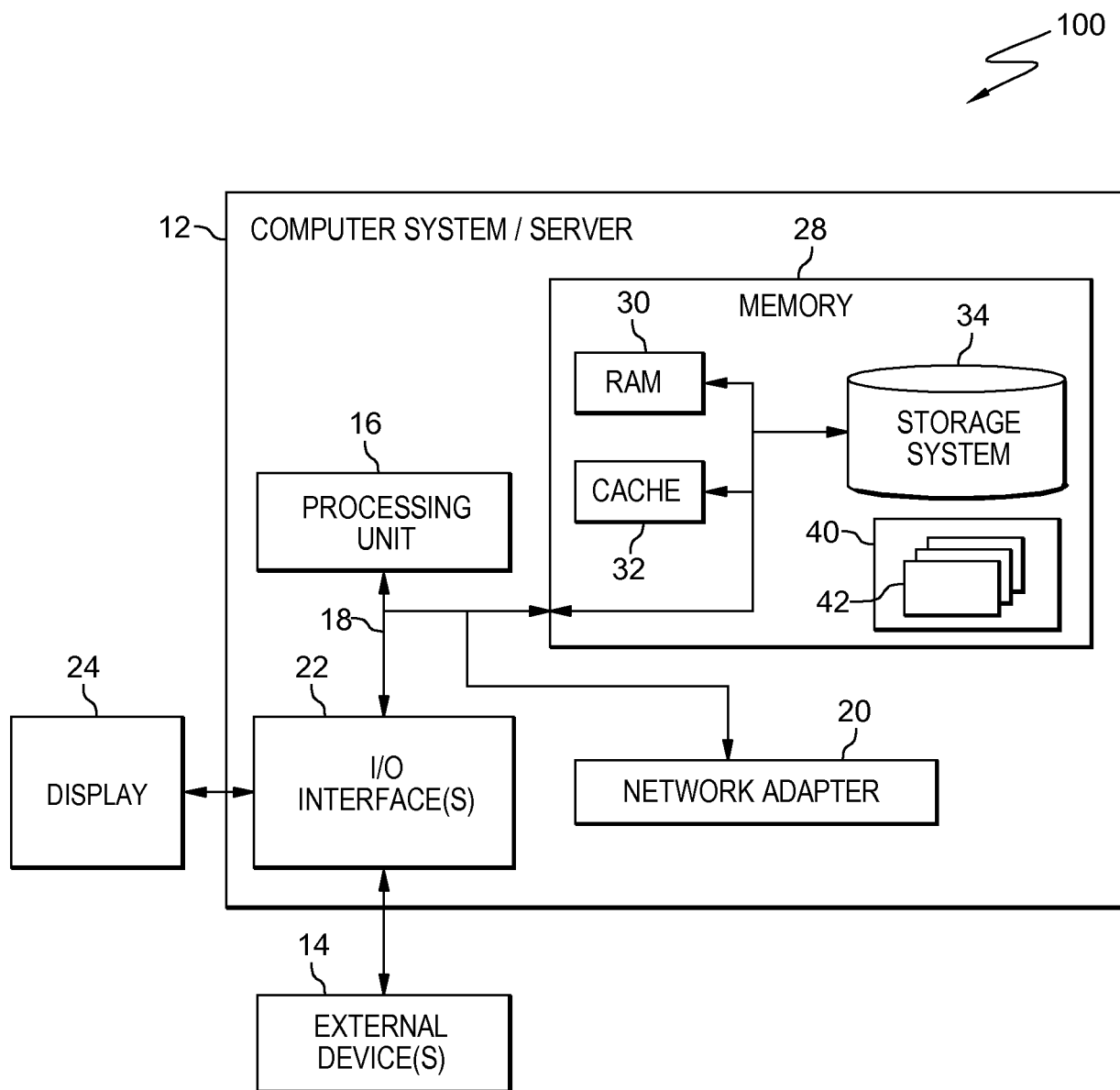
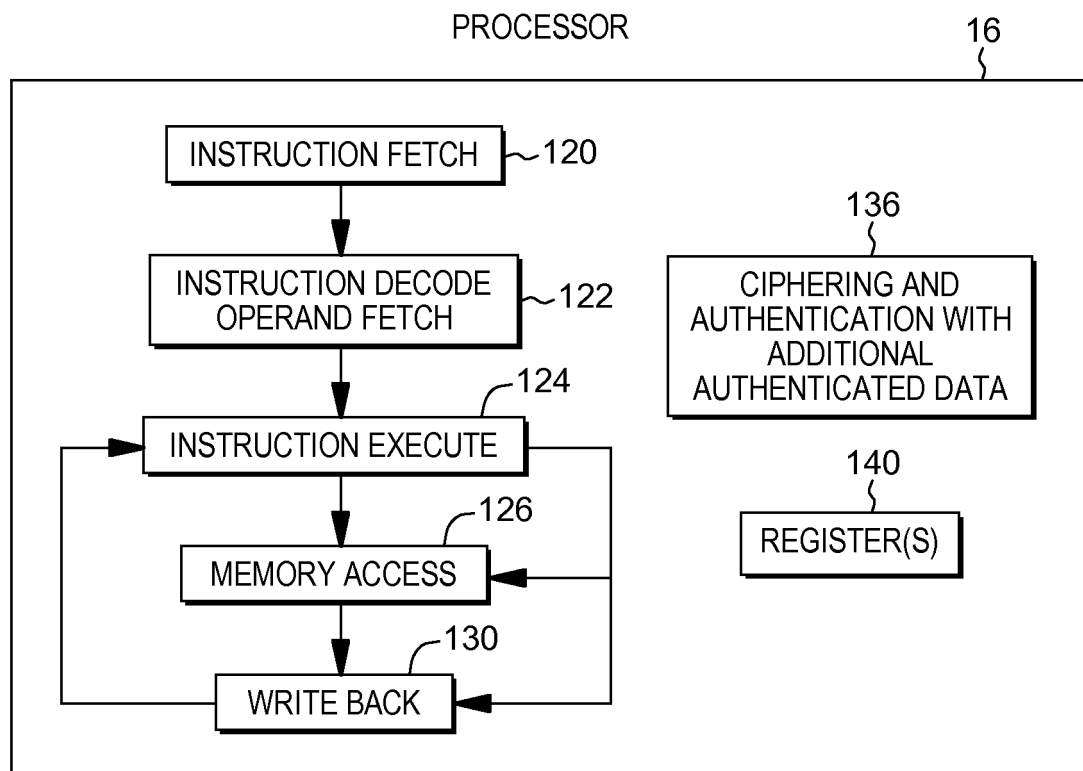


FIG. 1A



3/20

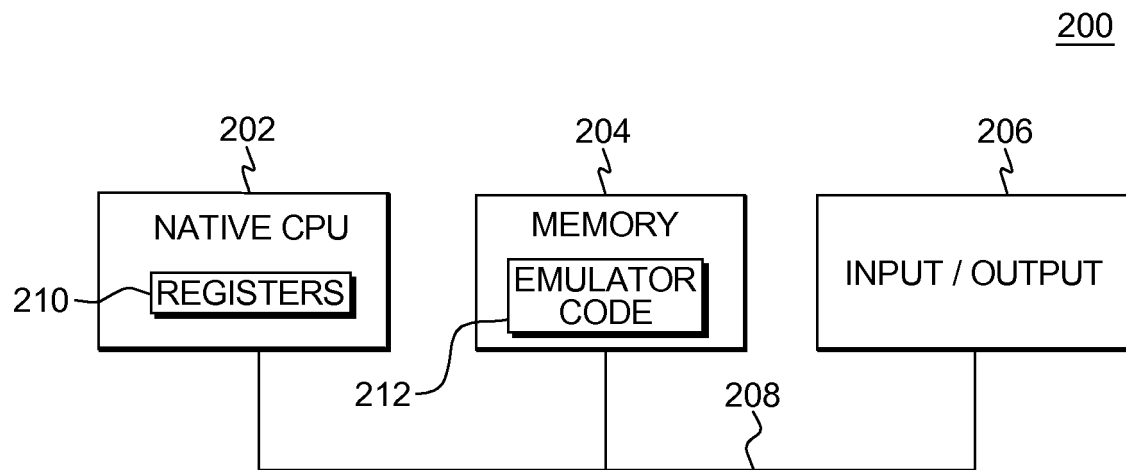


FIG. 2A

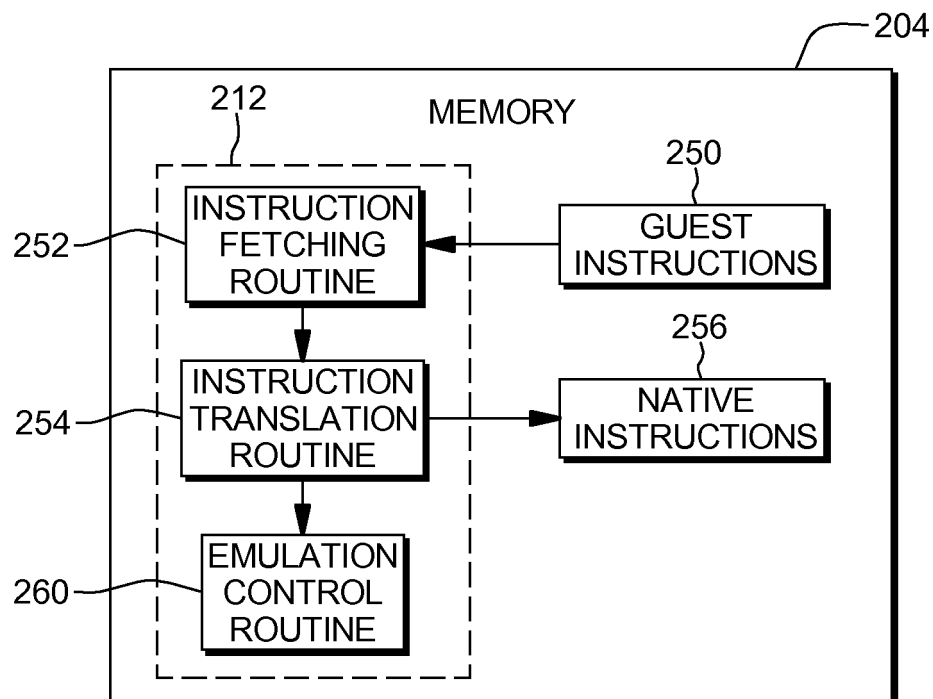


FIG. 2B

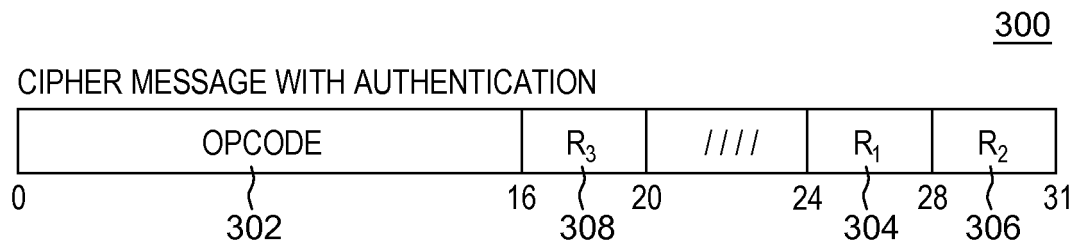


FIG. 3A

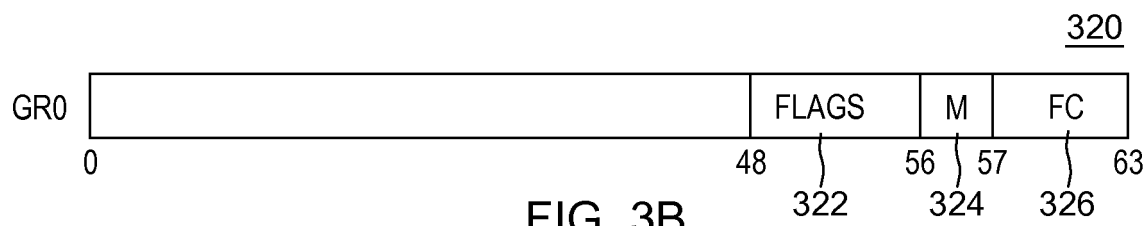


FIG. 3B

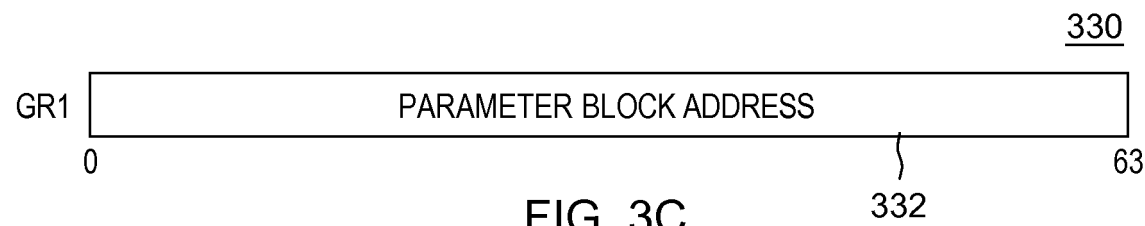


FIG. 3C

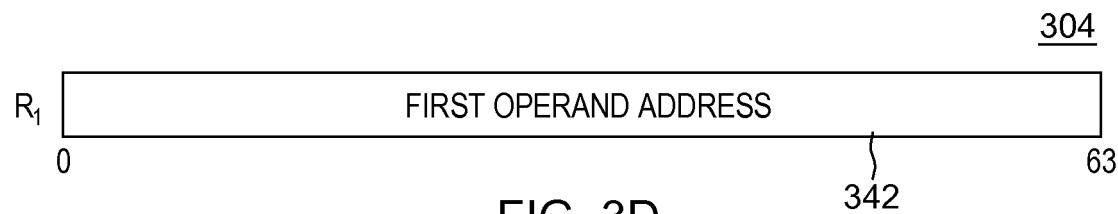


FIG. 3D

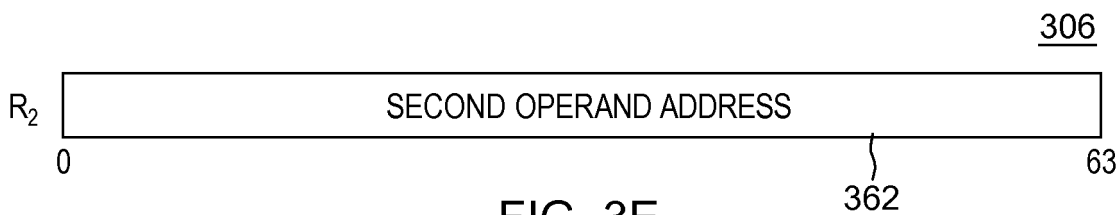


FIG. 3E

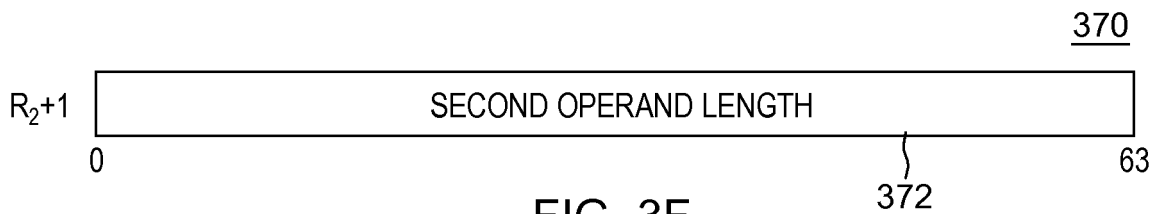
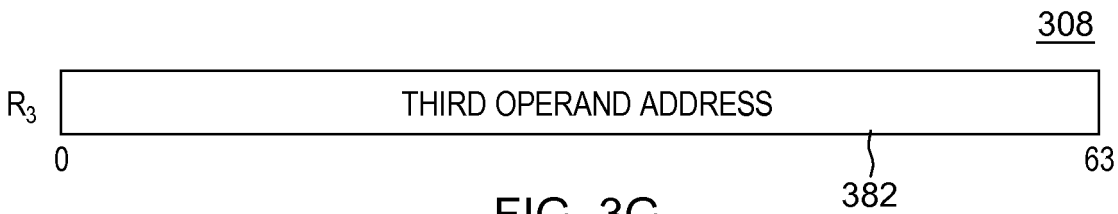
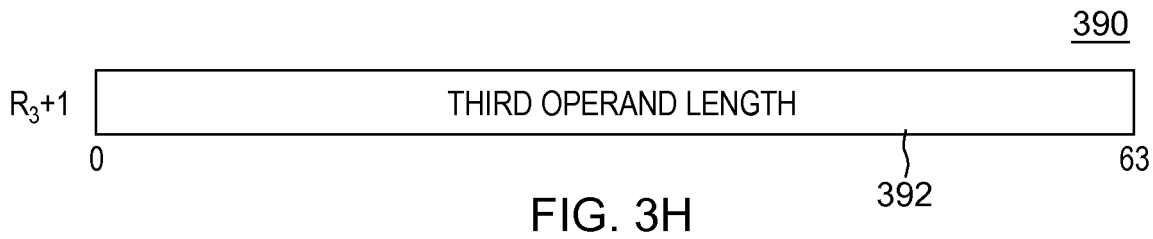


FIG. 3F



400

RESERVED		
RESERVED	COUNTER VALUE (CV)	~ 402
TAG (T)		~ 404
HASH SUBKEY (H)		~ 406
TOTAL AAD LENGTH (TAADL)		~ 408
TOTAL PLAINTEXT / CIPHERTEXT LENGTH (TPCL)		~ 410
INITIAL COUNTER VALUE (J_0)		~ 412
CRYPTOGRAPHIC KEY (K, FOR FUNCTIONS 18-20) ENCRYPTED CRYPTOGRAPHIC KEY ($WK_a(K)$, FOR FUNCTIONS 26-28)		~ 414
AES WRAPPING-KEY VERIFICATION PATTERN (WK_aVP) (PRESENT FOR FUNCTIONS 26-28)		~ 418

FIG. 4

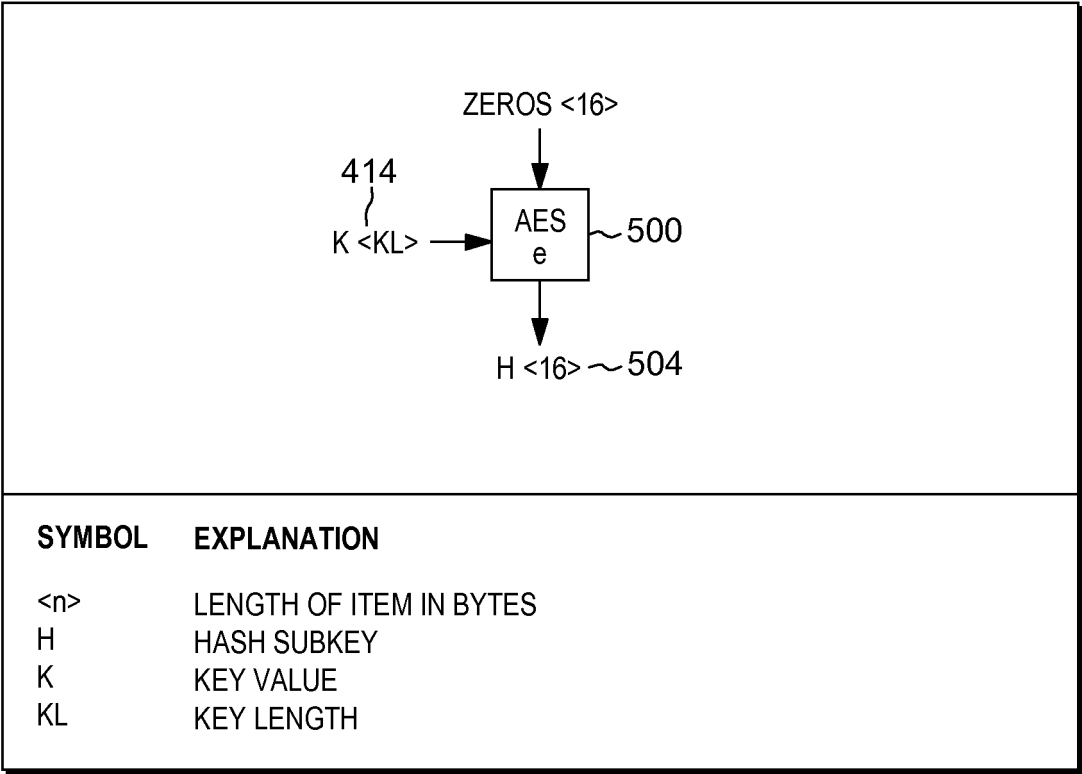


FIG. 5A

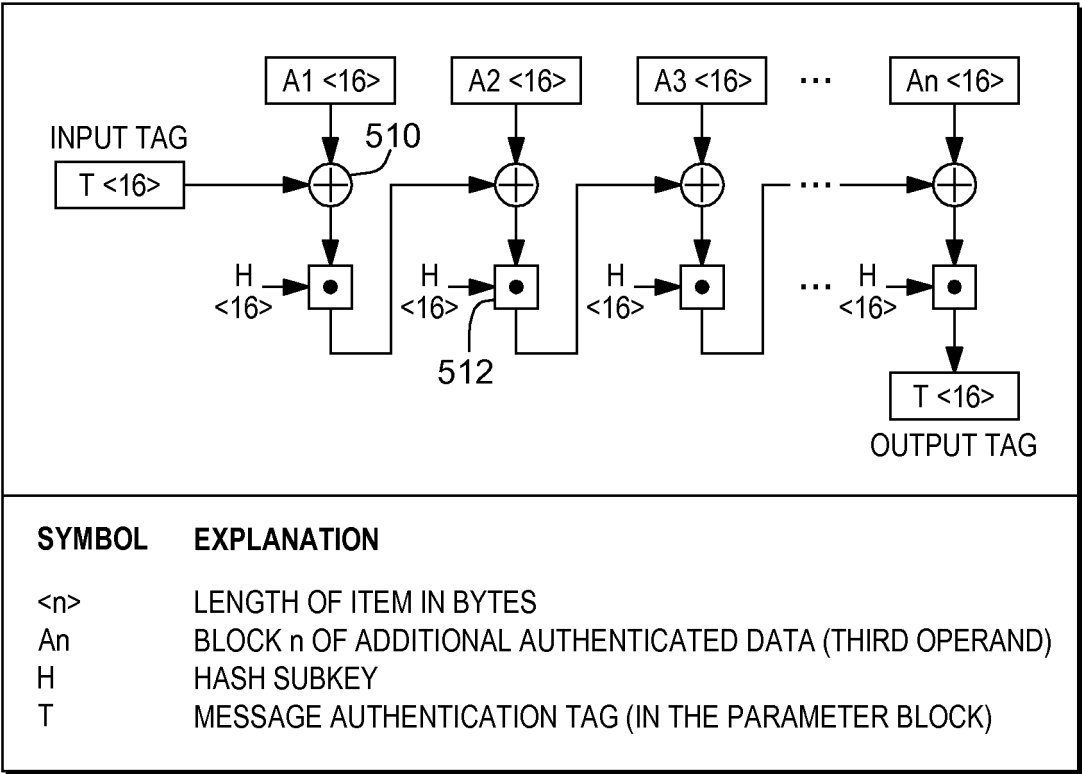


FIG. 5B

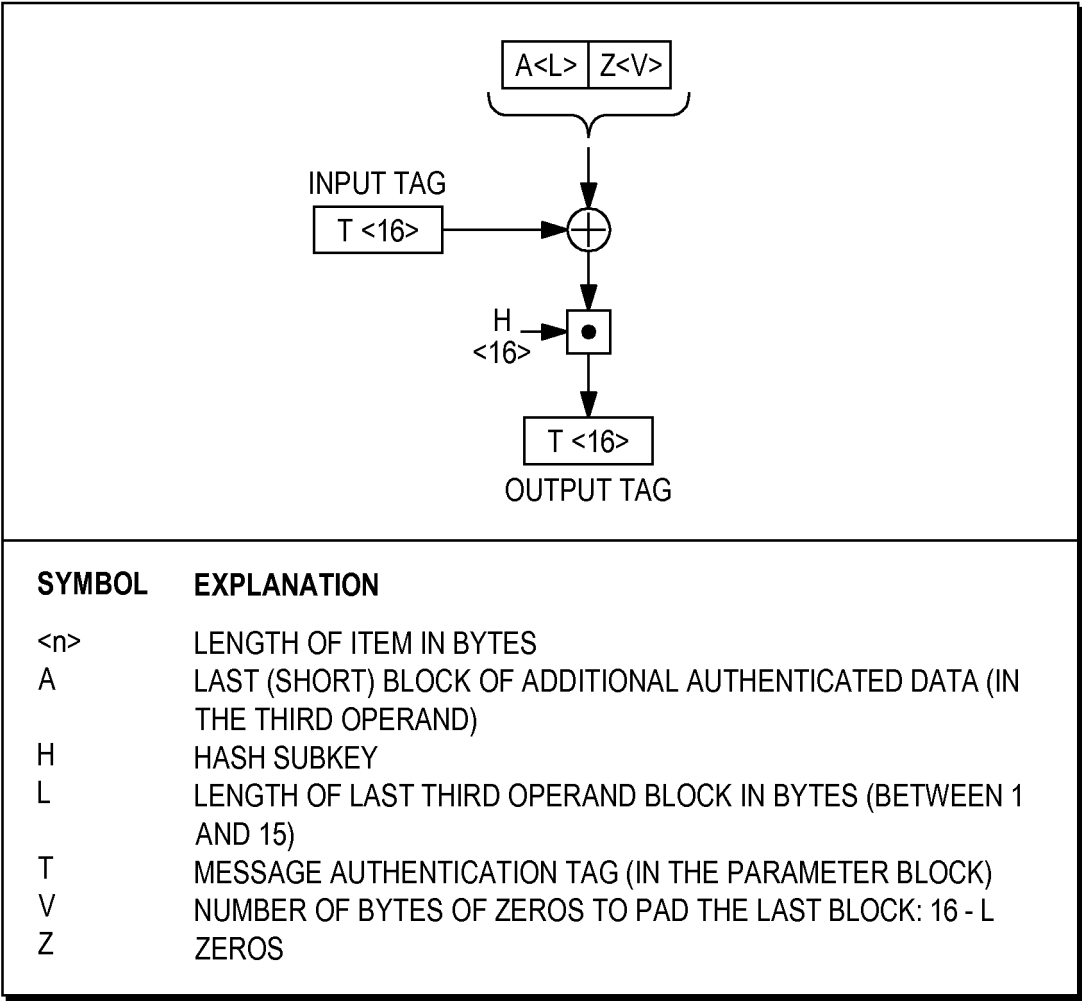


FIG. 5C

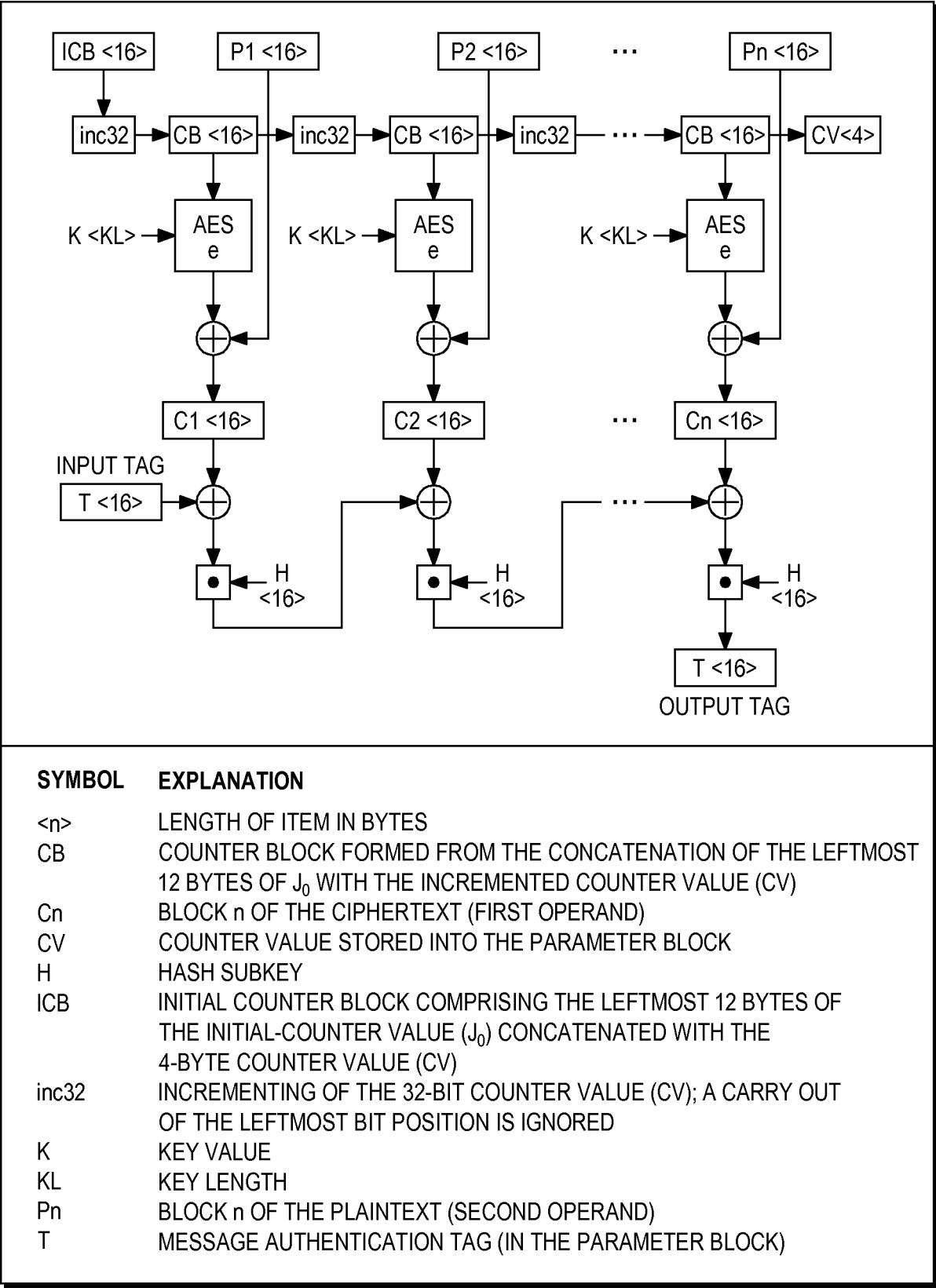


FIG. 5D

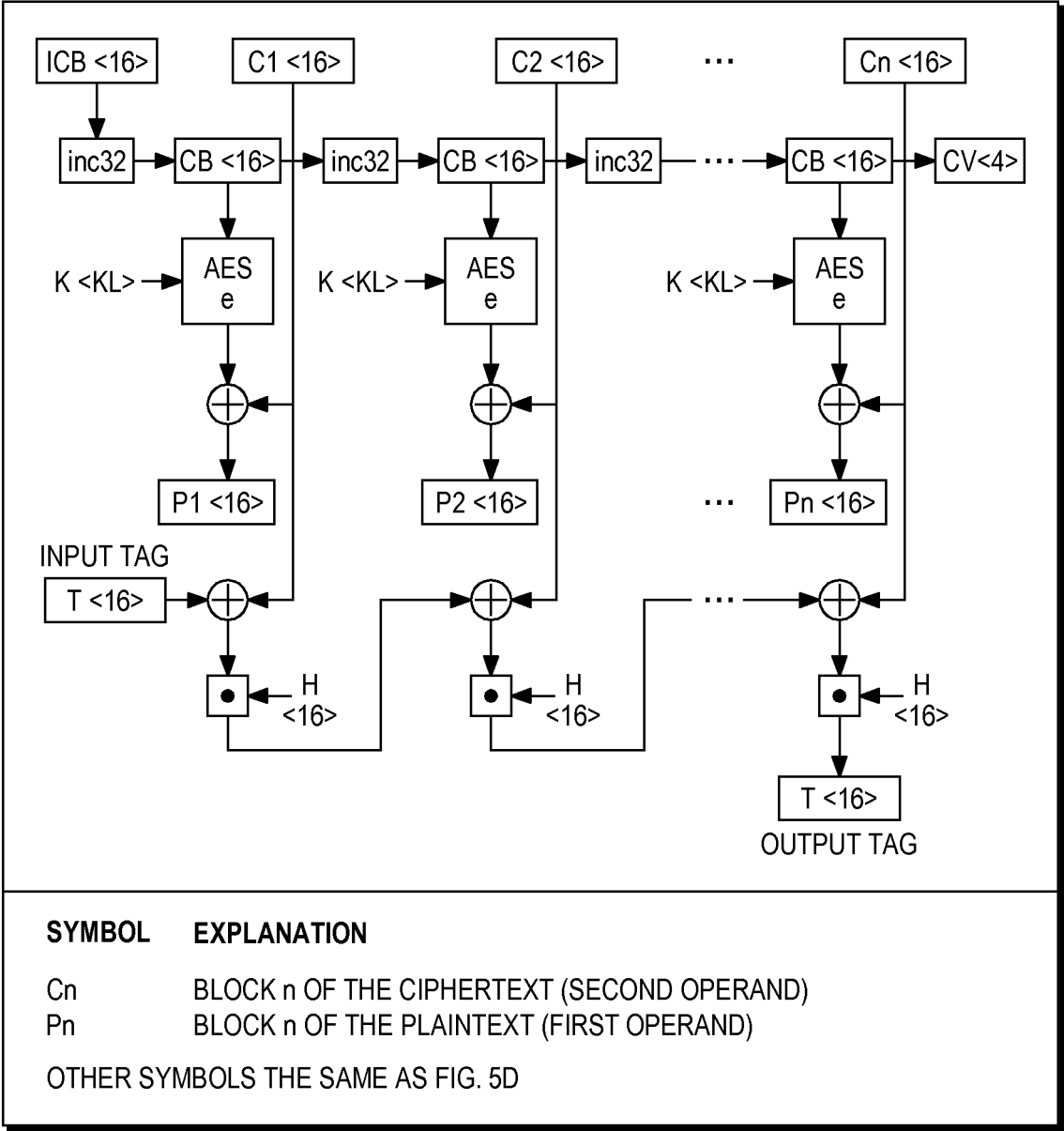


FIG. 5E

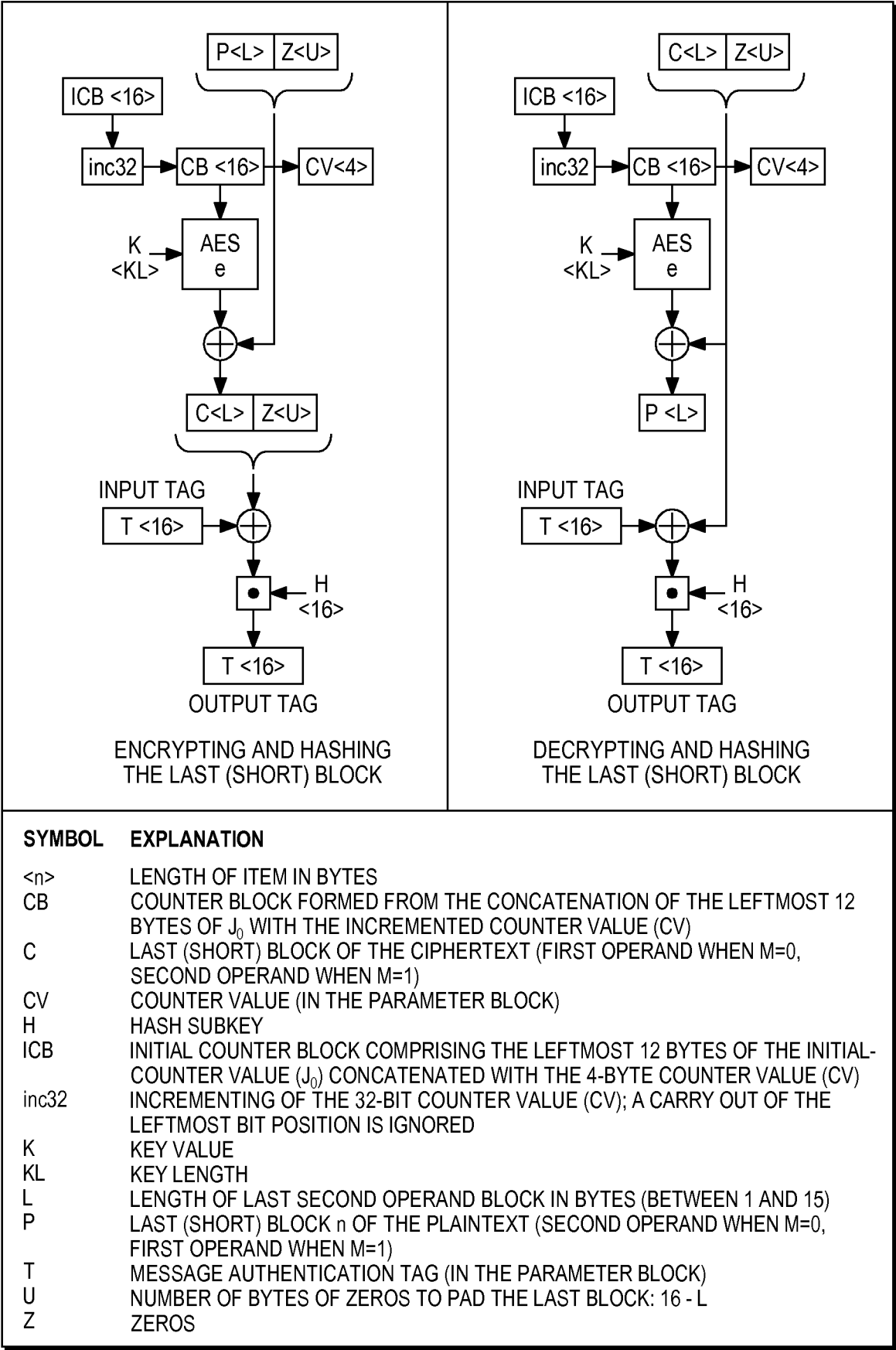


FIG. 5F

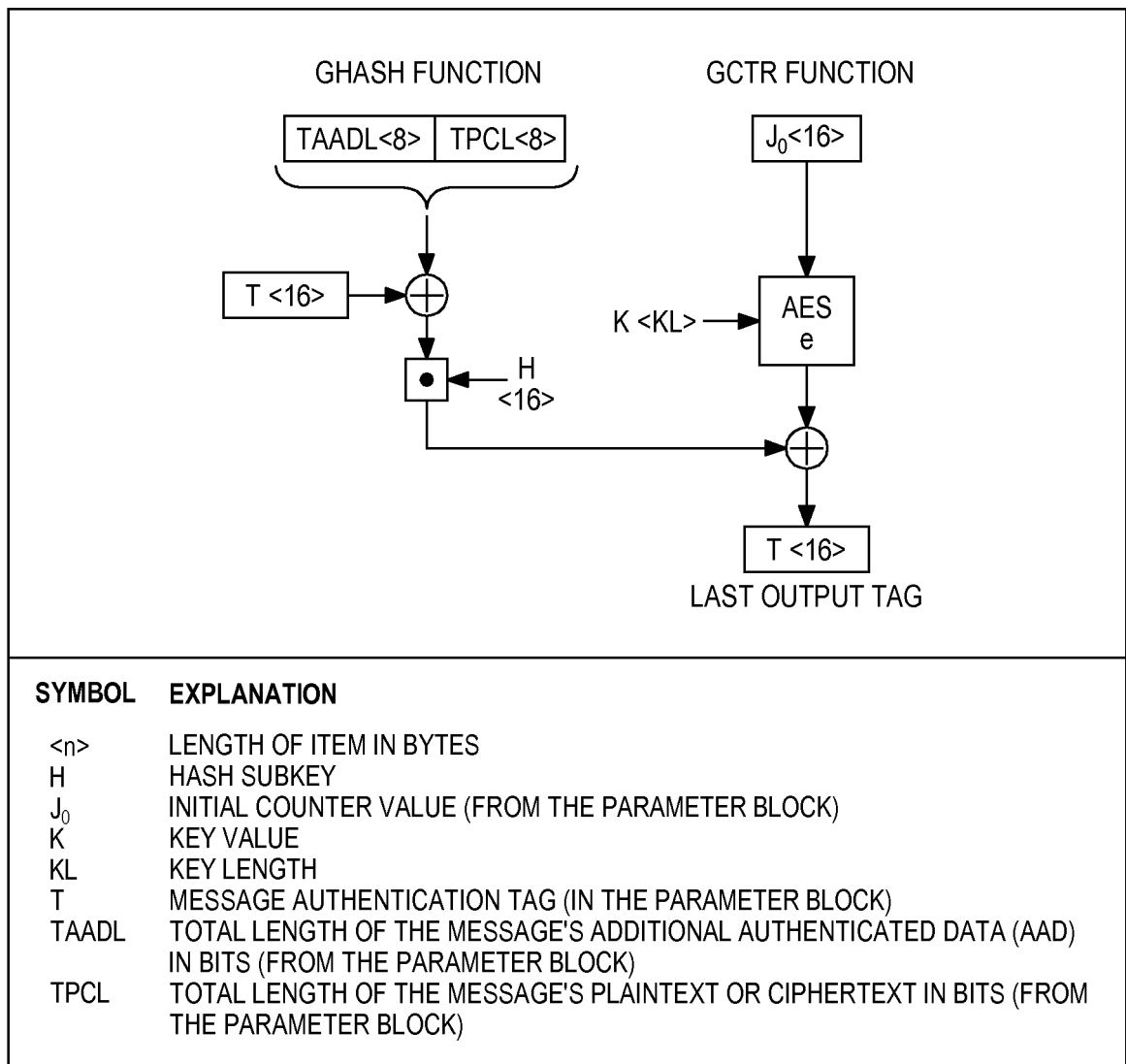


FIG. 5G

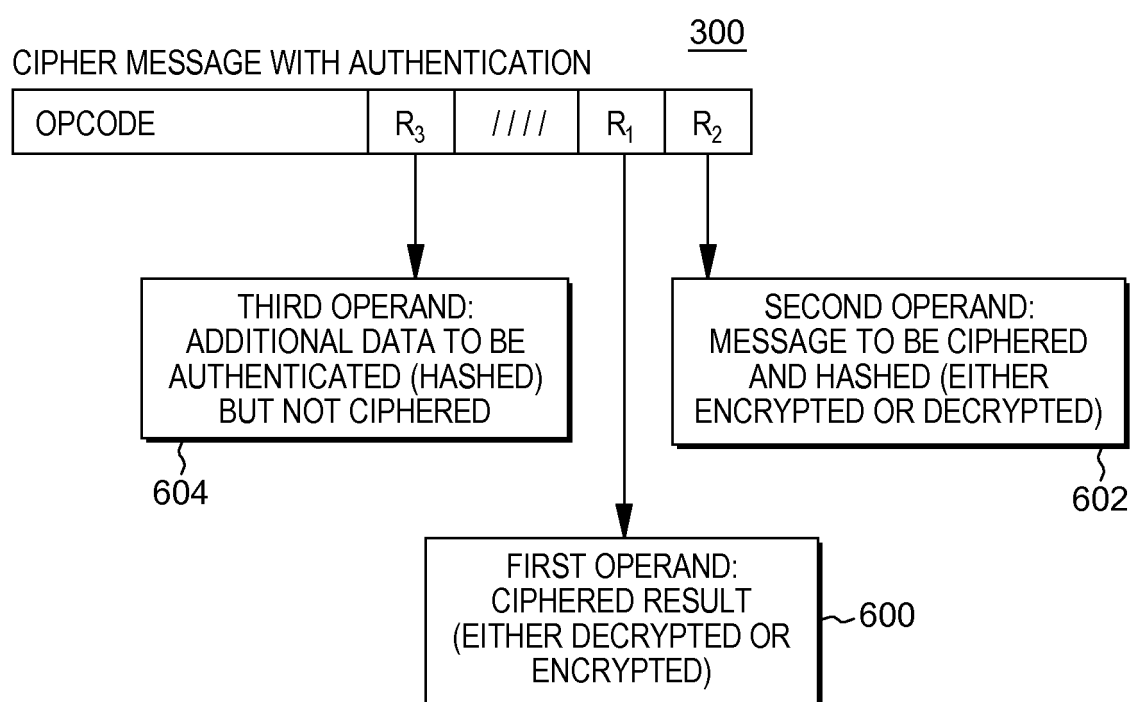


FIG. 6

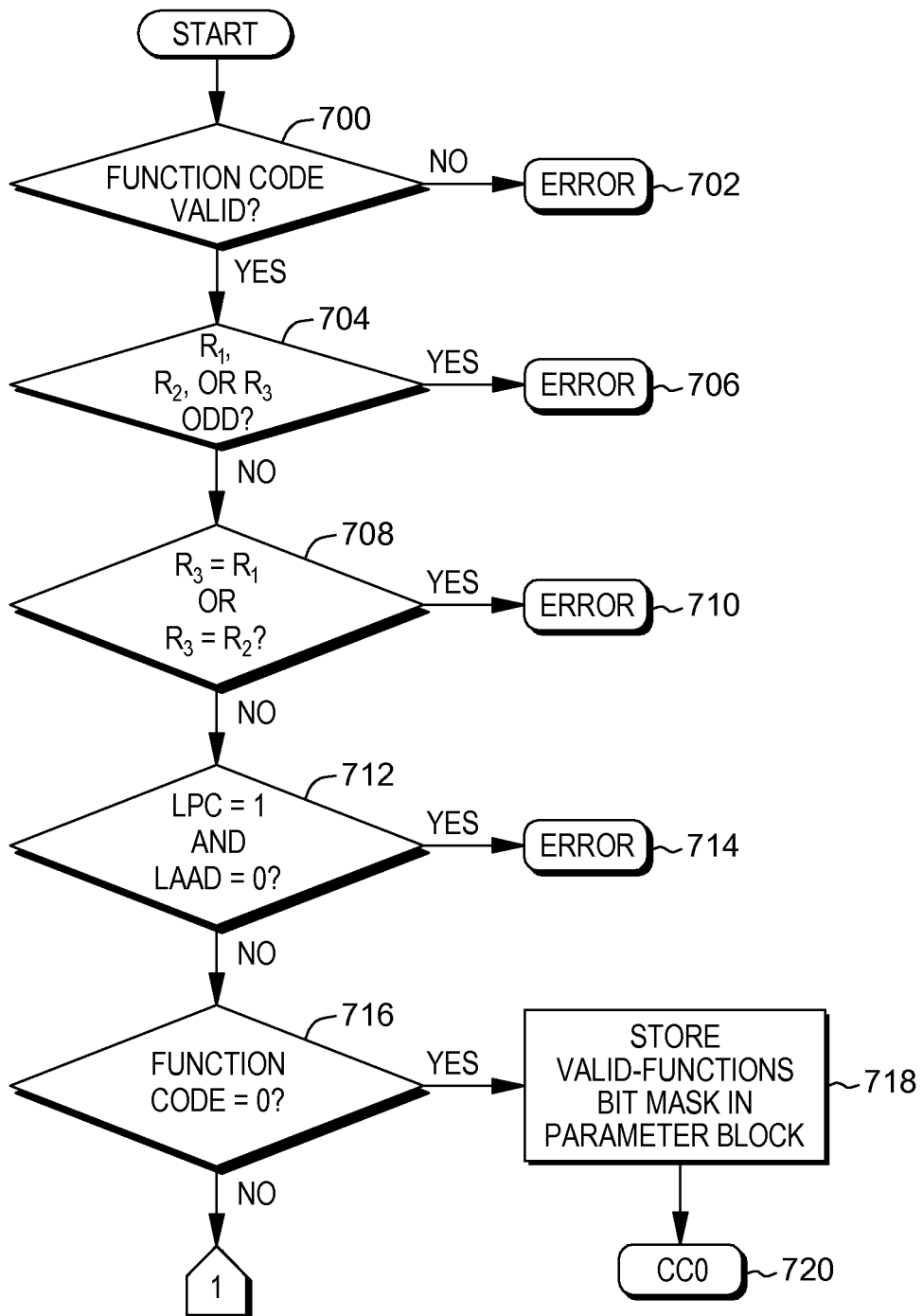


FIG. 7A

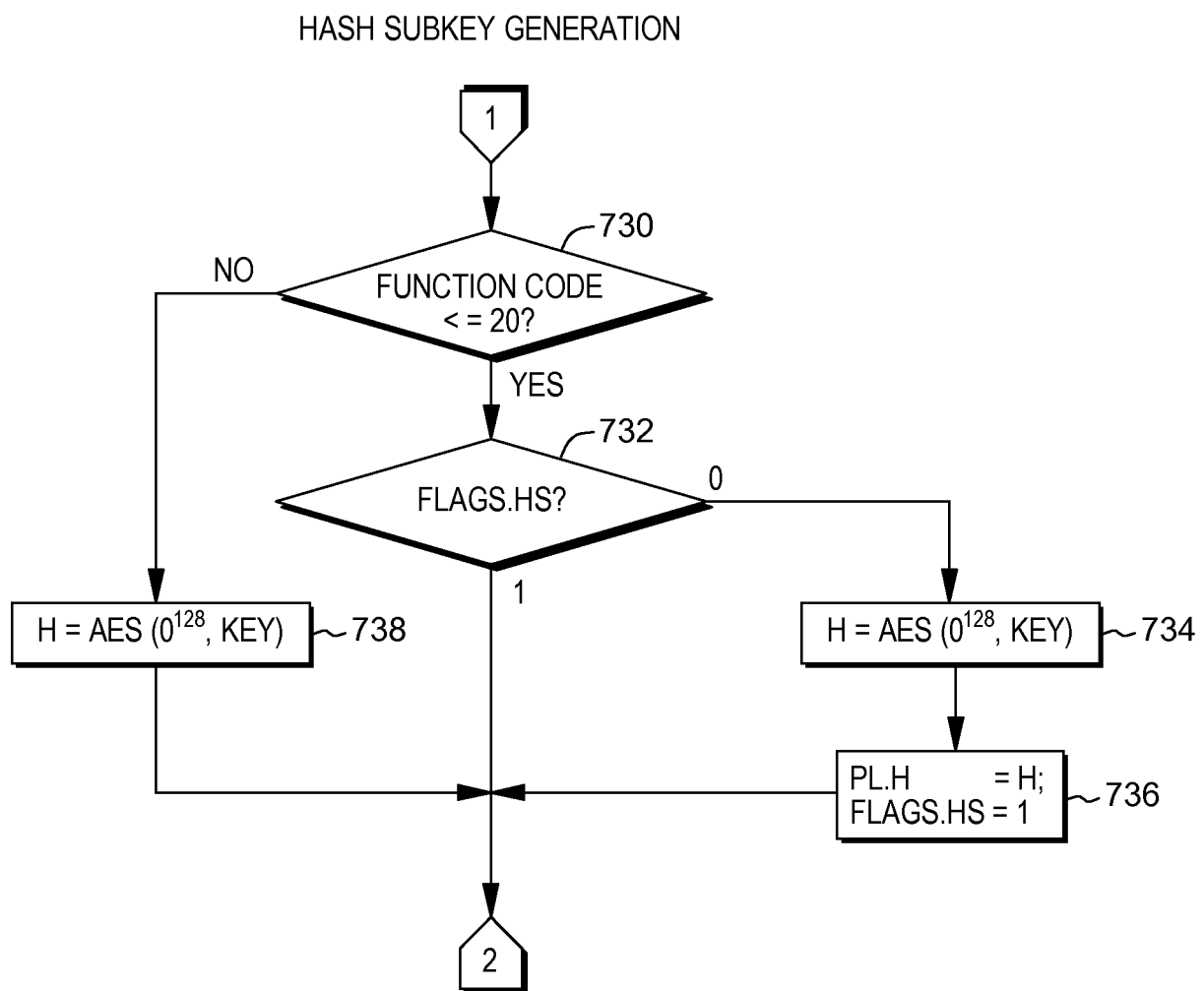
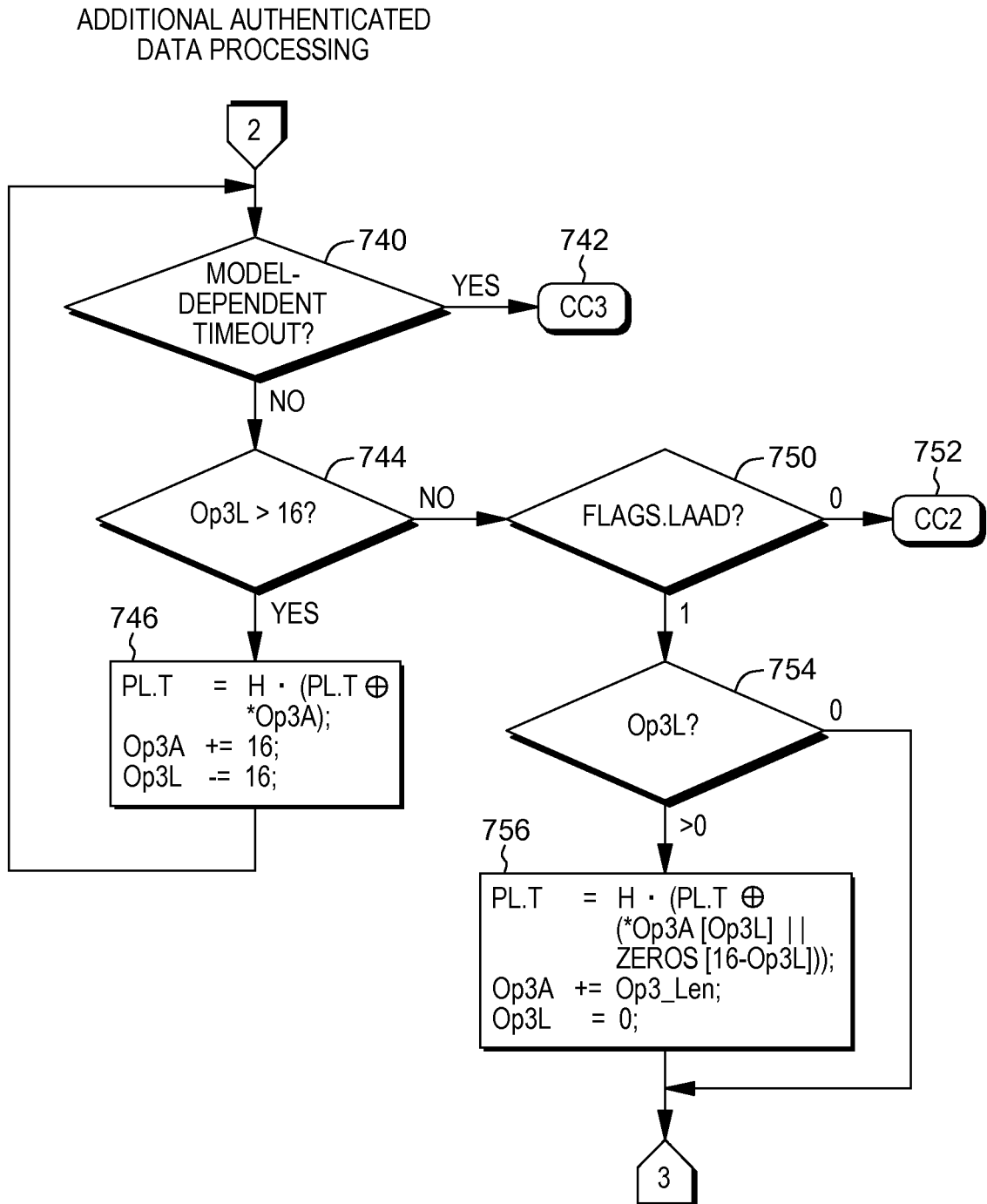


FIG. 7B



PLAINTEXT / CIPHER PROCESSING

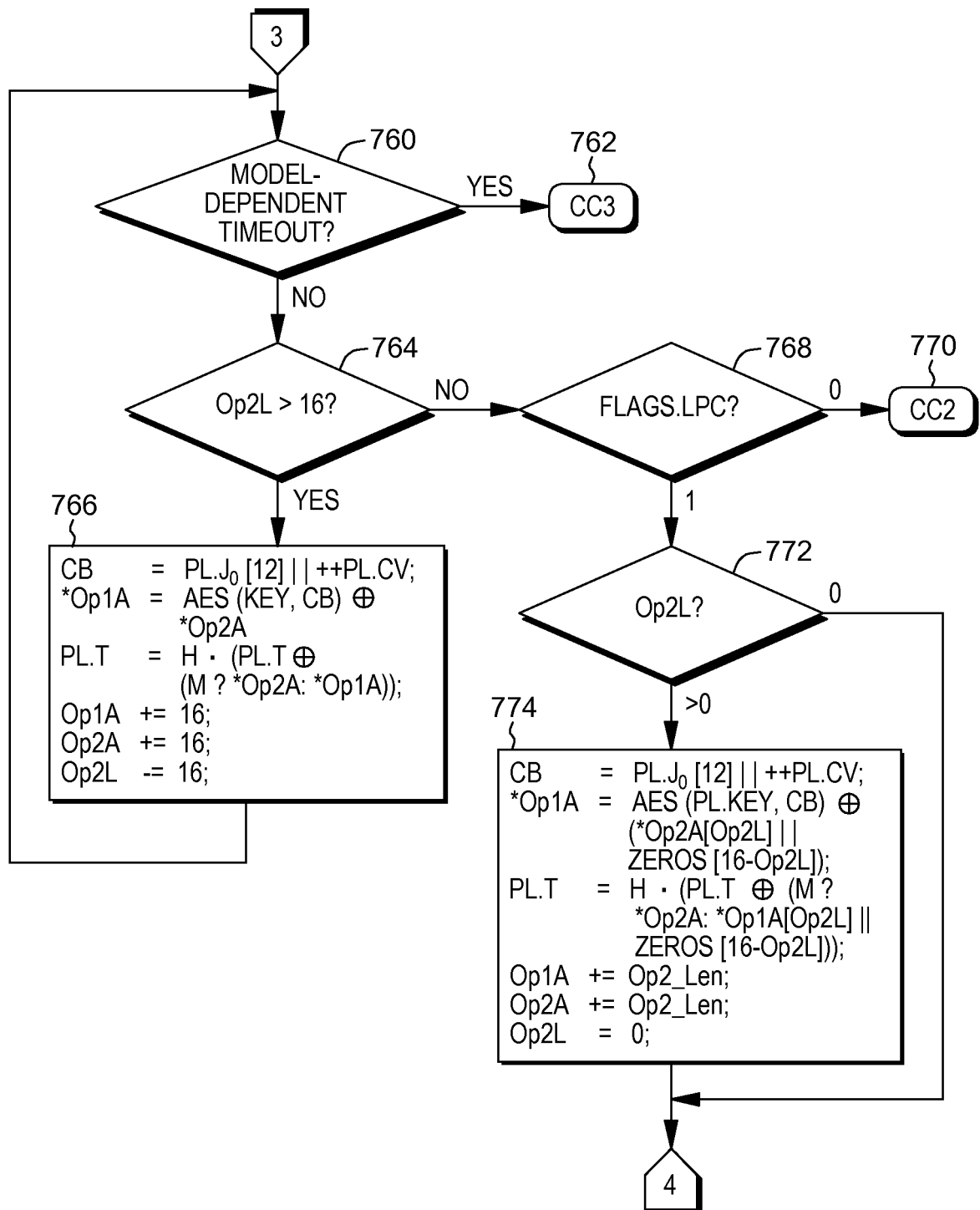


FIG. 7D

FINAL TAG PROCESSING

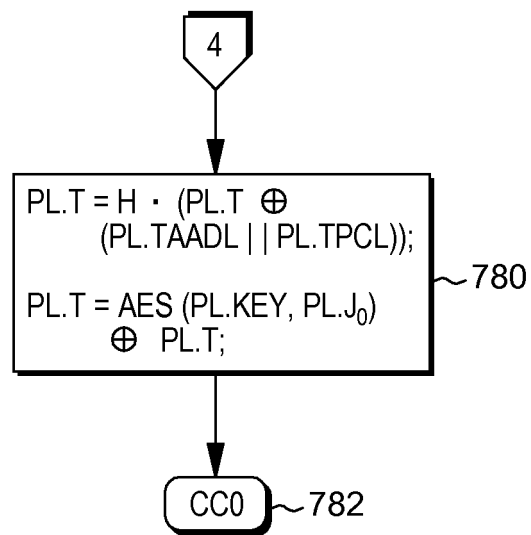


FIG. 7E

19/20

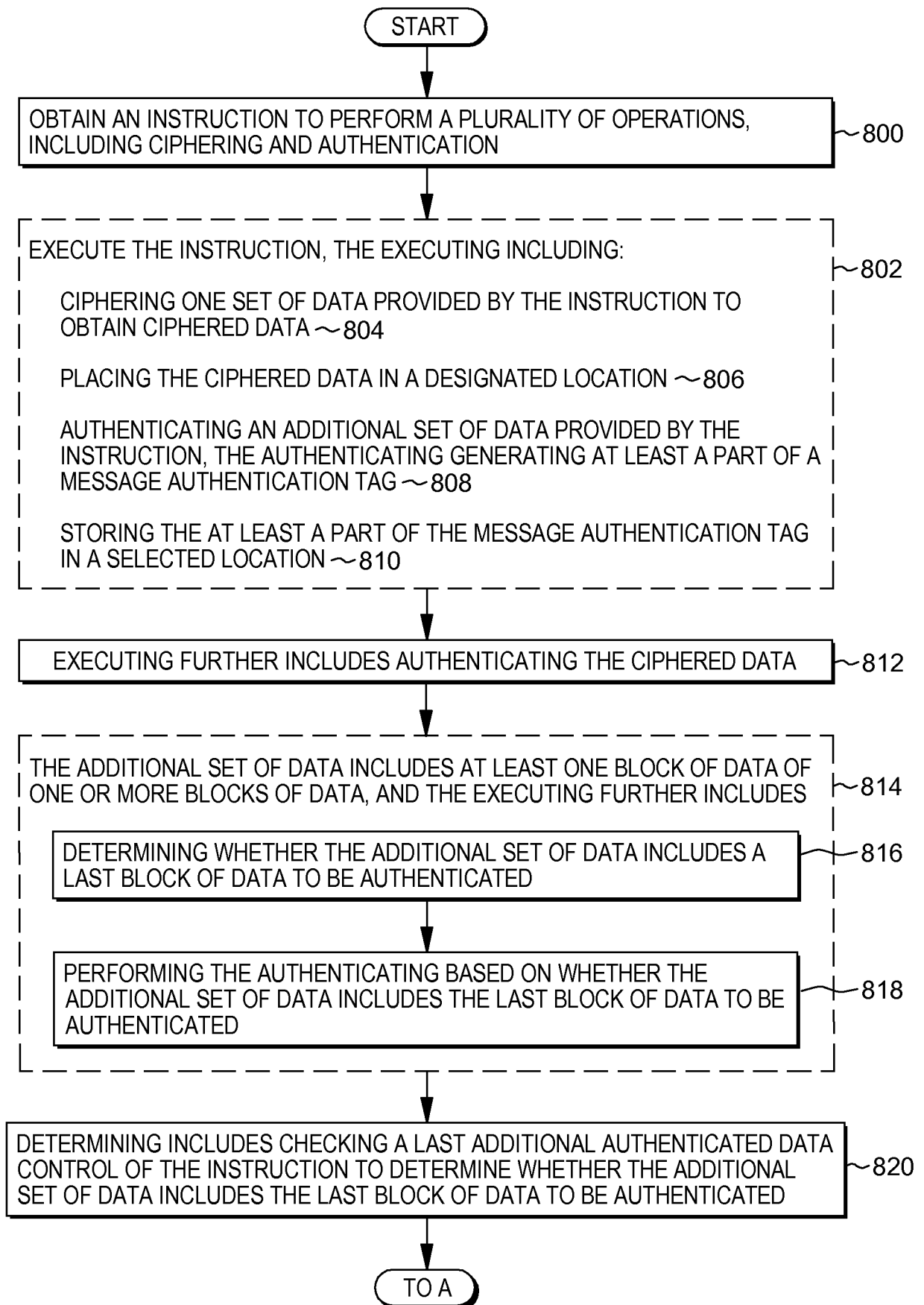


FIG. 8A

20/20

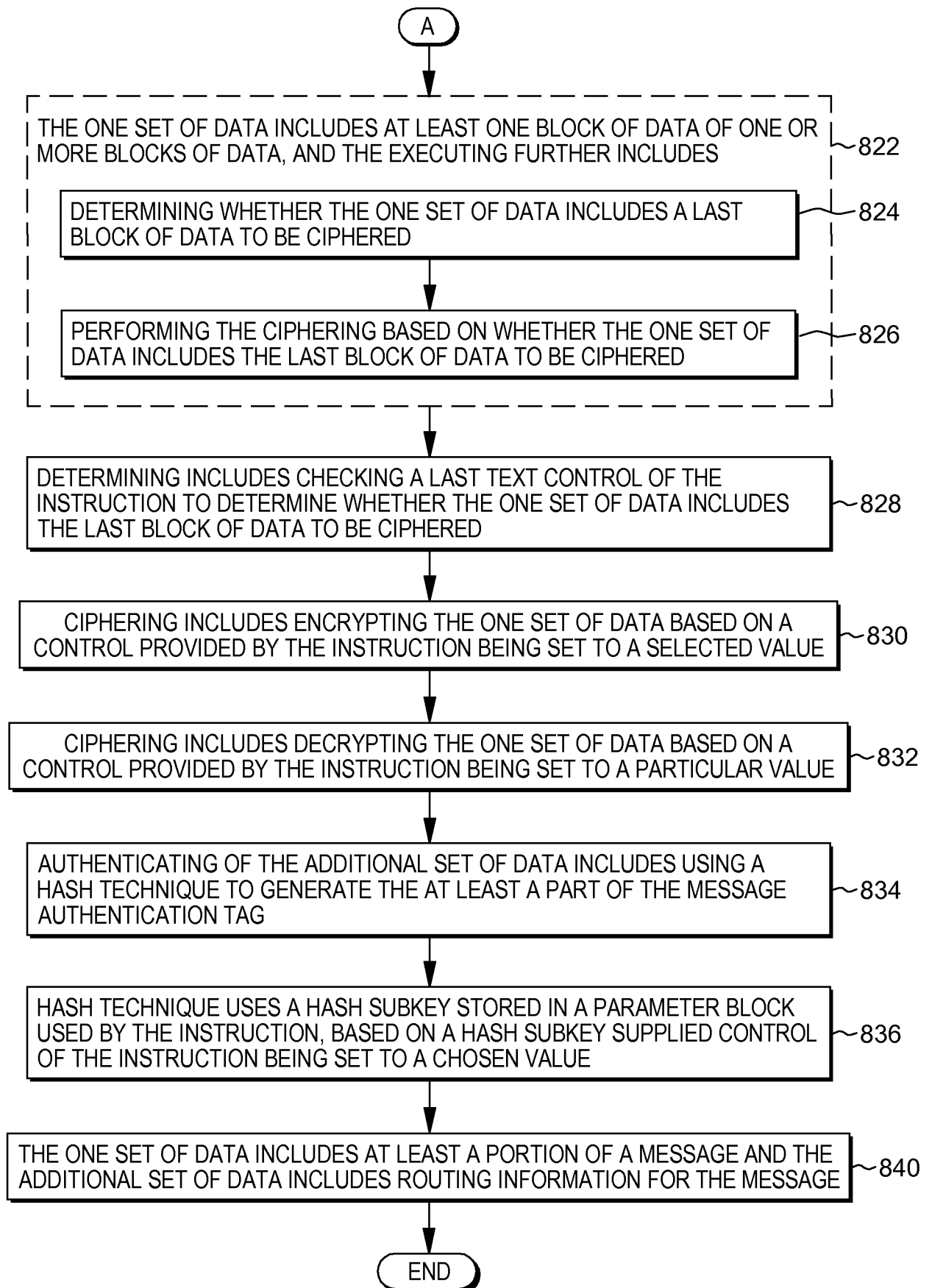


FIG. 8B