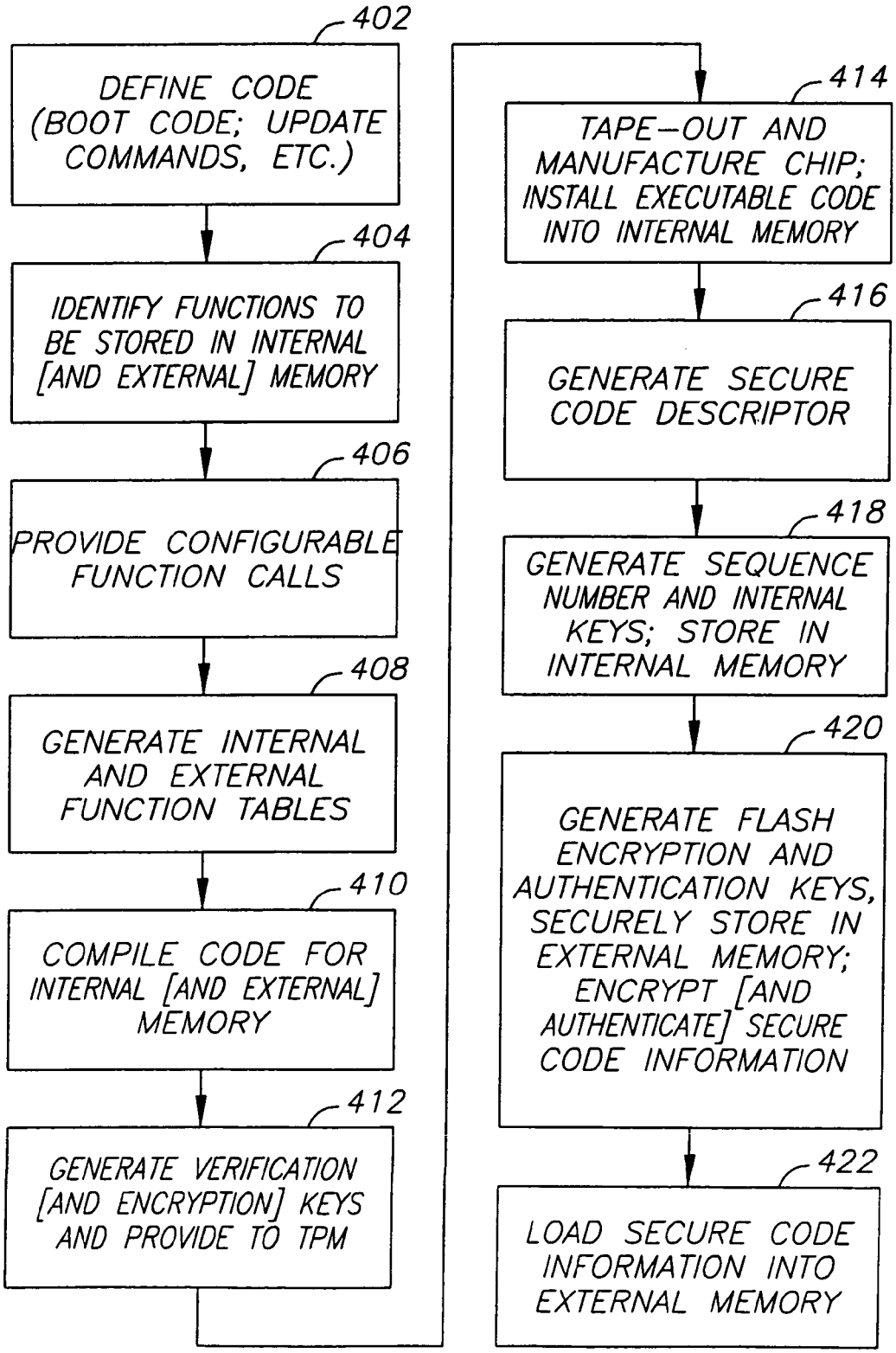
FIG. 4


402
DEFINE CODE (BOOT CODE; UPDATE COMMANDS, ETC.)
404
IDENTIFY FUNCTIONS TO BE STORED IN INTERNAL [AND EXTERNAL] MEMORY
406
PROVIDE CONFIGURABLE FUNCTION CALLS
408
GENERATE INTERNAL AND EXTERNAL FUNCTION TABLES
410
COMPILE CODE FOR INTERNAL [AND EXTERNAL] MEMORY
412
GENERATE VERIFICATION [AND ENCRYPTION] KEYS AND PROVIDE TO TPM
414
TAPE-OUT AND MANUFACTURE CHIP; INSTALL EXECUTABLE CODE INTO INTERNAL MEMORY
416
GENERATE SECURE CODE DESCRIPTOR
418
GENERATE SEQUENCE NUMBER AND INTERNAL KEYS; STORE IN INTERNAL MEMORY
420
GENERATE FLASH ENCRYPTION AND AUTHENTICATION KEYS, SECURELY STORE IN EXTERNAL MEMORY; ENCRYPT [AND AUTHENTICATE] SECURE CODE INFORMATION
422
LOAD SECURE CODE INFORMATION INTO EXTERNAL MEMORY