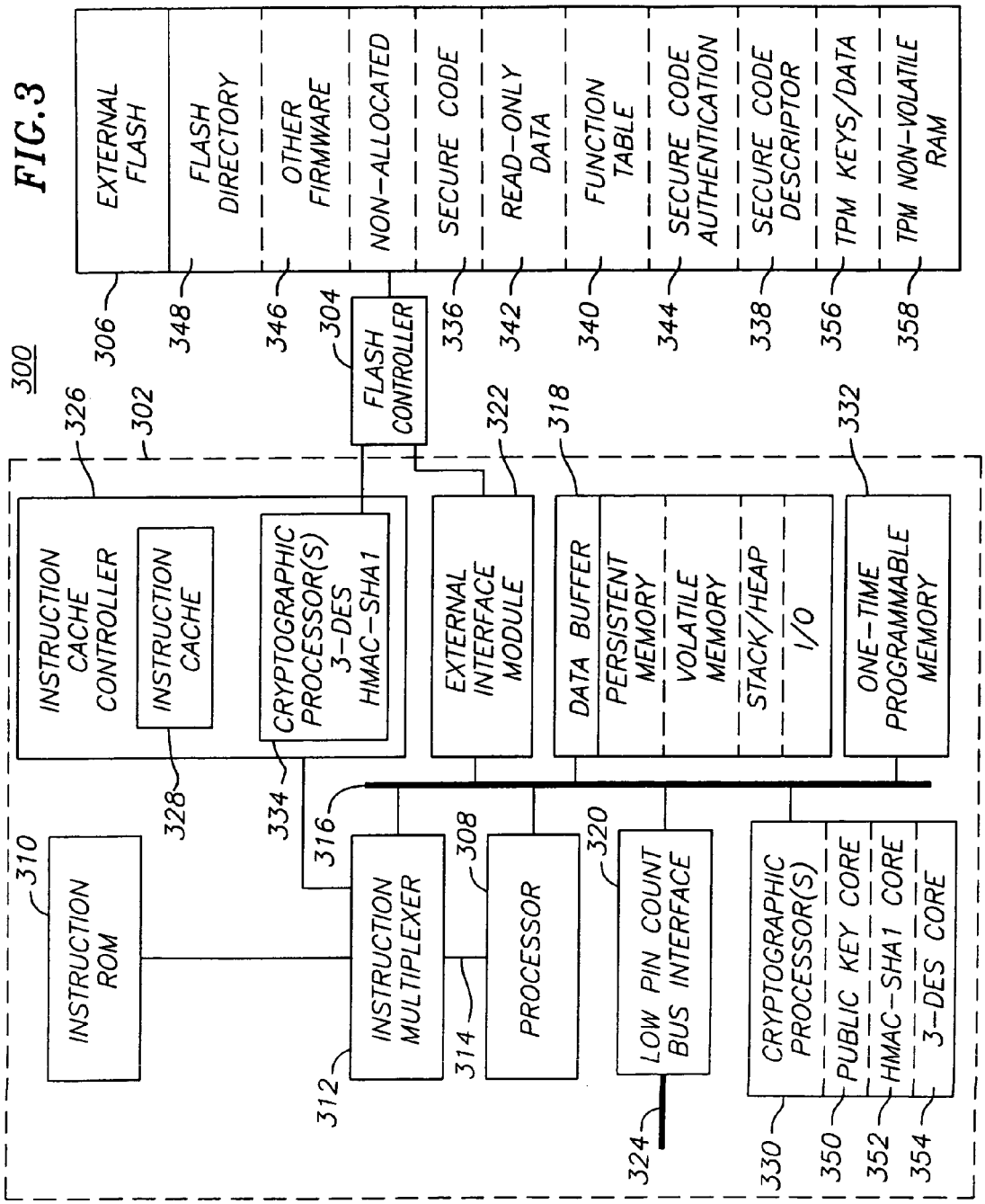
300
302
EXTERNAL FLASH
FLASH DIRECTORY
OTHER FIRMWARE
NON-ALLOCATED
SECURE CODE
READ-ONLY DATA
FUNCTION TABLE
SECURE CODE AUTHENTICATION
SECURE CODE DESCRIPTOR
TPM KEYS/DATA
TPM NON-VOLATILE RAM
306
348
346
304
336
342
340
344
338
356
358
FLASH CONTROLLER
322
318
332
326
INSTRUCTION CACHE CONTROLLER
INSTRUCTION CACHE
CRYPTOGRAPHIC PROCESSOR(S) 3-DES HMAC-SHA1
EXTERNAL INTERFACE MODULE
DATA BUFFER
PERSISTENT MEMORY
VOLATILE MEMORY
STACK/HEAP
I/O
ONE-TIME PROGRAMMABLE MEMORY
328
334
316
310
308
320
INSTRUCTION ROM
INSTRUCTION MULTIPLEXER
PROCESSOR
LOW PIN COUNT BUS INTERFACE
CRYPTOGRAPHIC PROCESSOR(S)
PUBLIC KEY CORE
HMAC-SHA1 CORE
3-DES CORE
312
314
324
330
350
352
354

FIG. 3