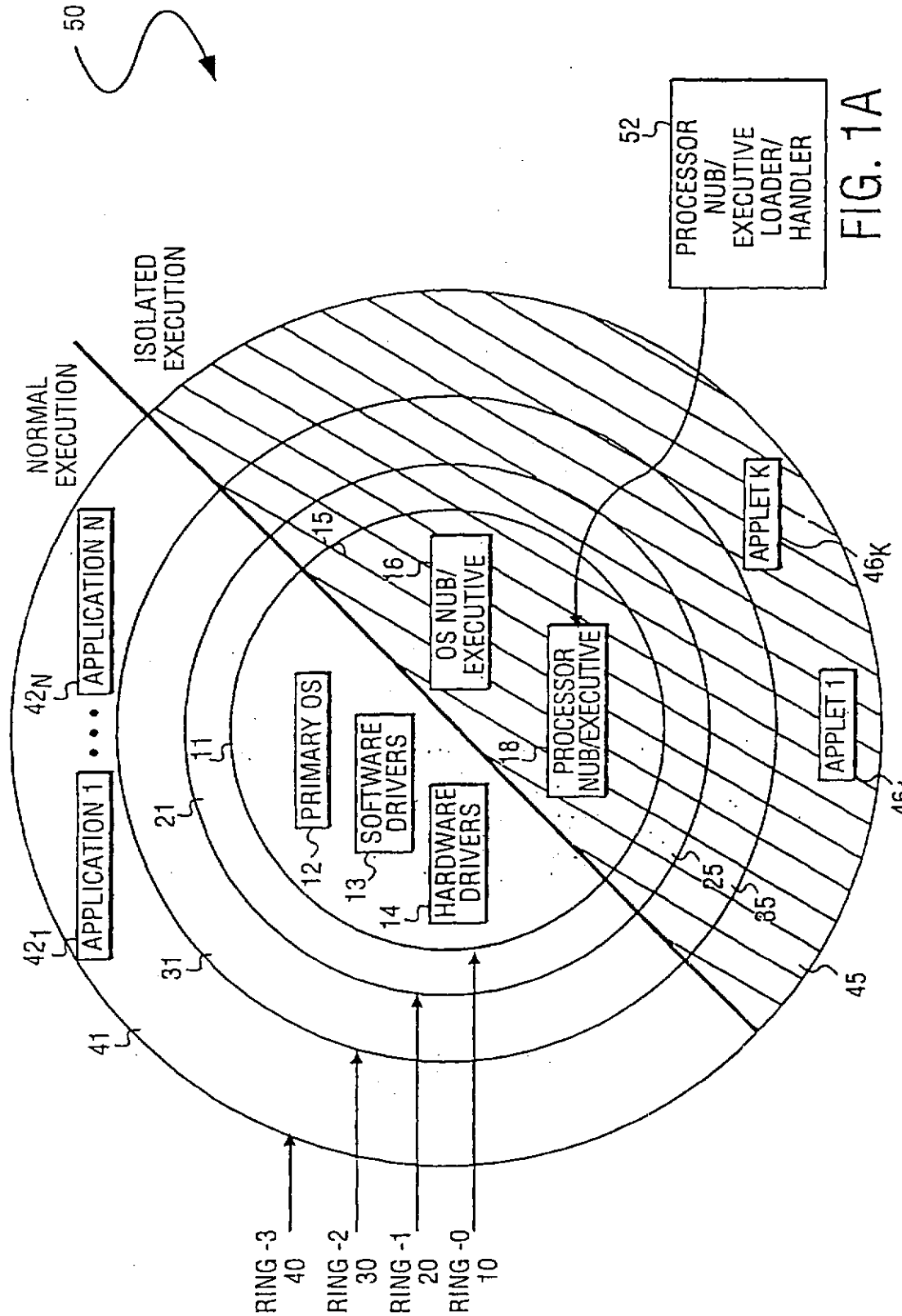

50
NORMAL EXECUTION
ISOLATED EXECUTION
PROCESSOR NUB/ EXECUTIVE LOADER/ HANDLER
52
APPLICATION N
APPLICATION 1
42N
421
PRIMARY OS
SOFTWARE DRIVERS
HARDWARE DRIVERS
OS NUB/ EXECUTIVE
PROCESSOR NUB/EXECUTIVE
APPLET K
APPLET 1
46K
461
11
12
13
14
15
16
18
21
25
31
35
41
45
RING -3 40
RING -2 30
RING -1 20
RING -0 10

FIG. 1A

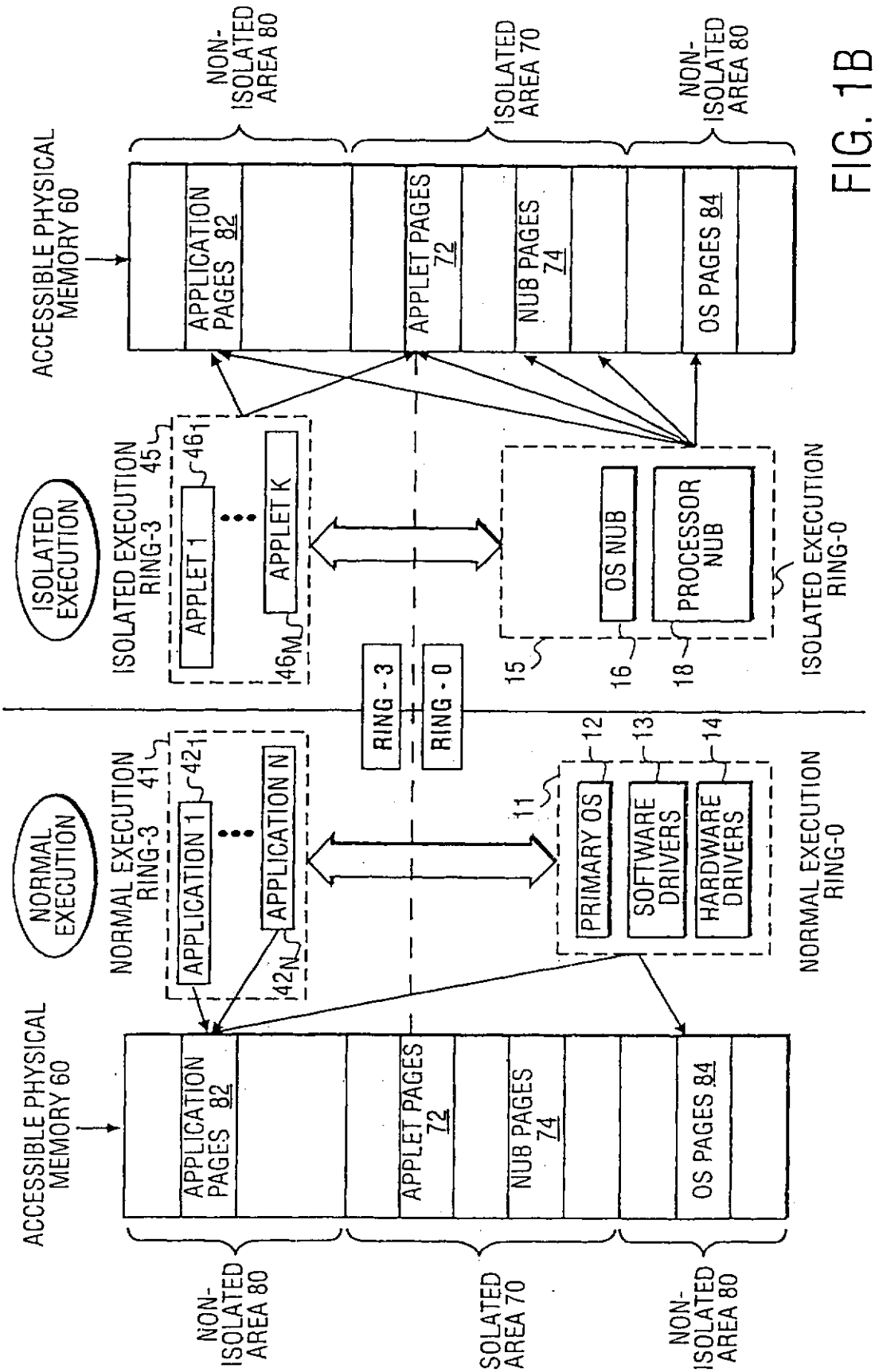

ACCESSIBLE PHYSICAL MEMORY 60
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
ISOLATED EXECUTION
ISOLATED EXECUTION RING-3 45
APPLET 1
461
APPLET K
46M
OS NUB
PROCESSOR NUB
ISOLATED EXECUTION RING-0
15
16
18
RING - 3
RING - 0
NORMAL EXECUTION
NORMAL EXECUTION RING-3 41
APPLICATION 1
421
APPLICATION N
42N
11
PRIMARY OS
SOFTWARE DRIVERS
HARDWARE DRIVERS
12
13
14
NORMAL EXECUTION RING-0
ACCESSIBLE PHYSICAL MEMORY 60
APPLICATION PAGES 82
APPLET PAGES 72
NUB PAGES 74
OS PAGES 84
NON-ISOLATED AREA 80
ISOLATED AREA 70
NON-ISOLATED AREA 80

FIG. 1B

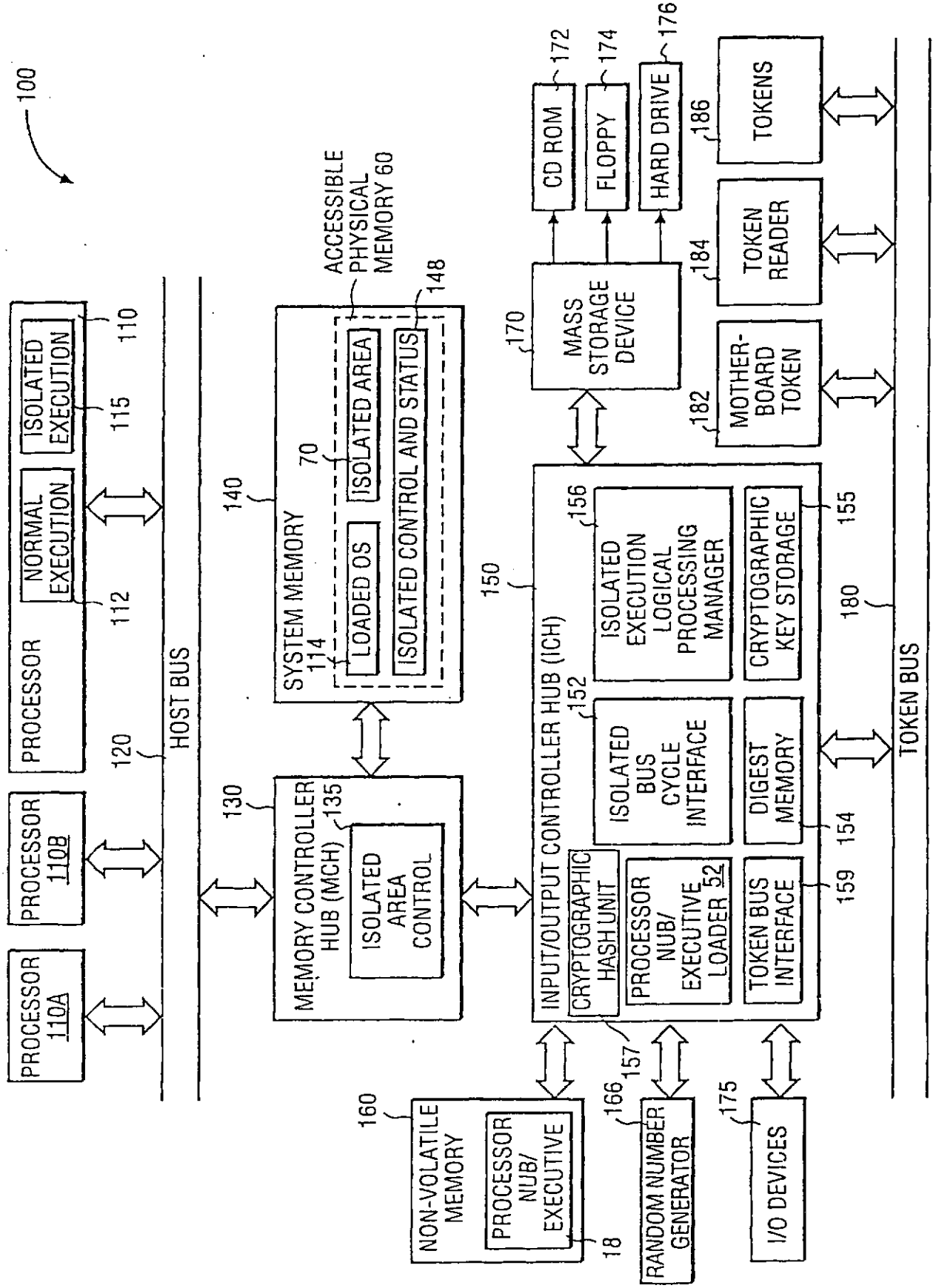

100
PROCESSOR 110A
PROCESSOR 110B
PROCESSOR
NORMAL EXECUTION
ISOLATED EXECUTION
110
112
115
120
HOST BUS
130
MEMORY CONTROLLER HUB (MCH)
135
ISOLATED AREA CONTROL
140
SYSTEM MEMORY 114
70
LOADED OS
ISOLATED AREA
ISOLATED CONTROL AND STATUS
148
ACCESSIBLE PHYSICAL MEMORY 60
150
INPUT/OUTPUT CONTROLLER HUB (ICH)
152
CRYPTOGRAPHIC HASH UNIT
PROCESSOR NUB/ EXECUTIVE LOADER 52
TOKEN BUS INTERFACE
159
ISOLATED BUS CYCLE INTERFACE
DIGEST MEMORY
154
156
ISOLATED EXECUTION LOGICAL PROCESSING MANAGER
CRYPTOGRAPHIC KEY STORAGE
155
180
TOKEN BUS
170
MASS STORAGE DEVICE
CD ROM
172
FLOPPY
174
HARD DRIVE
176
186
TOKENS
184
TOKEN READER
182
MOTHER-BOARD TOKEN
160
NON-VOLATILE MEMORY
PROCESSOR NUB/ EXECUTIVE
18
166
157
RANDOM NUMBER GENERATOR
175
I/O DEVICES

FIG. 1C

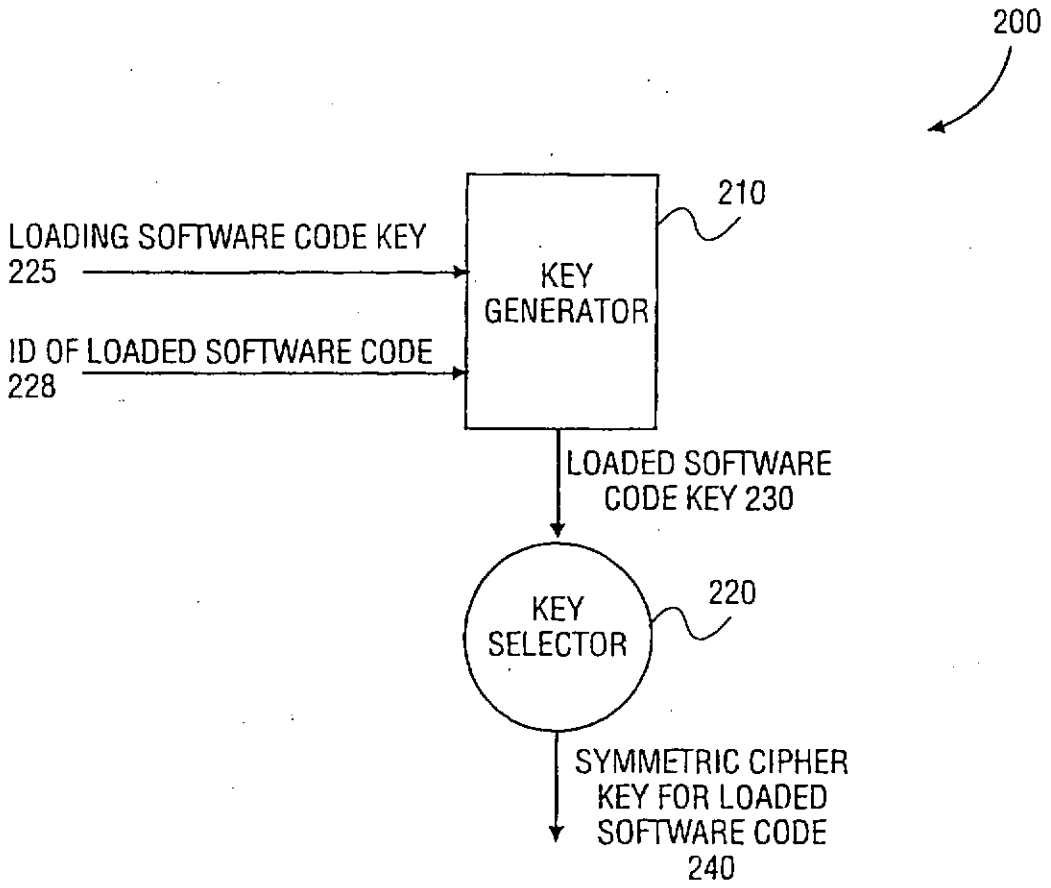

200
210
LOADING SOFTWARE CODE KEY
225
ID OF LOADED SOFTWARE CODE
228
KEY
GENERATOR
LOADED SOFTWARE
CODE KEY 230
220
KEY
SELECTOR
SYMMETRIC CIPHER
KEY FOR LOADED
SOFTWARE CODE
240

FIG. 2

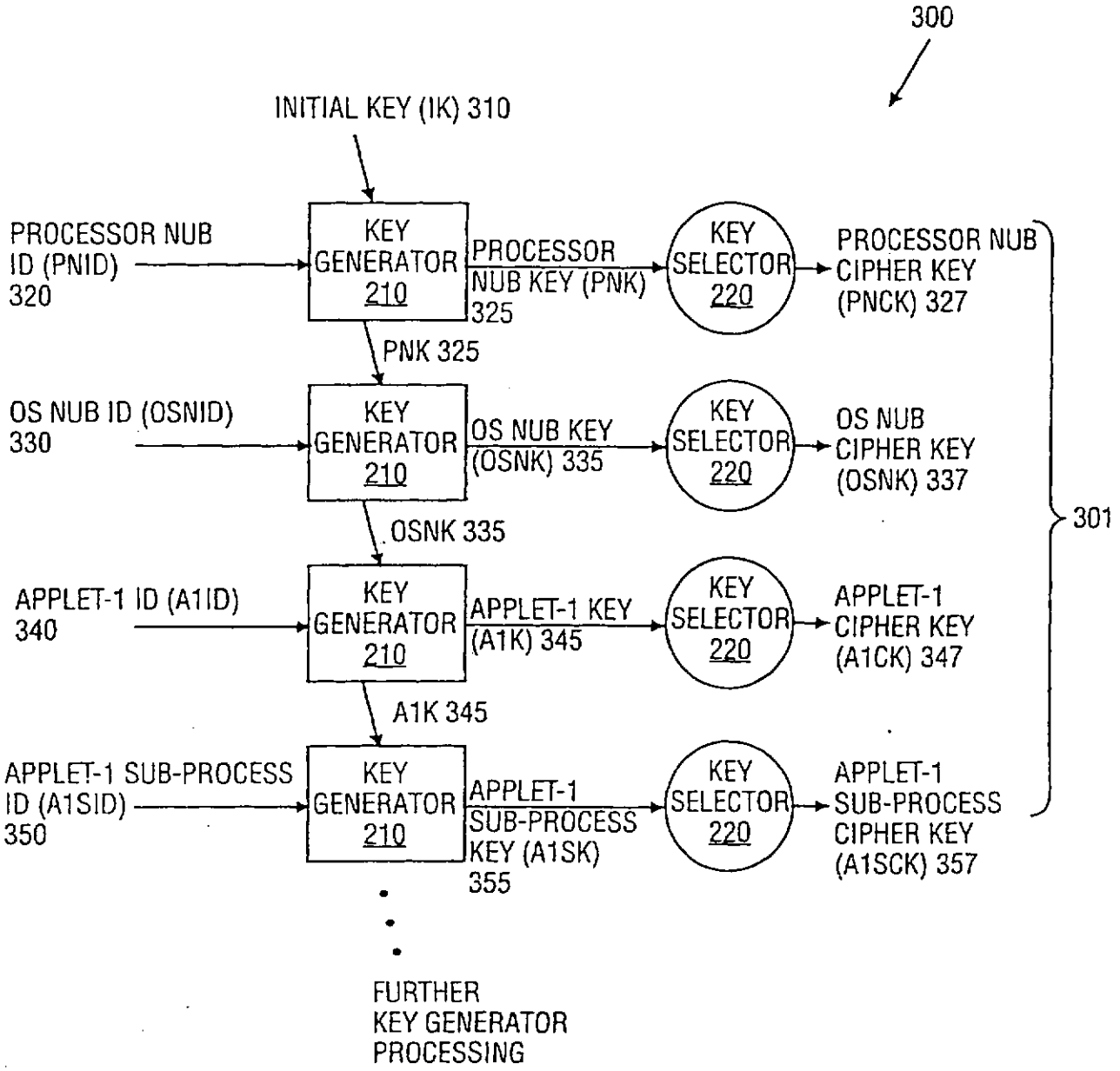

300
INITIAL KEY (IK) 310
PROCESSOR NUB ID (PNID) 320
KEY GENERATOR 210
PROCESSOR NUB KEY (PNK) 325
KEY SELECTOR 220
PROCESSOR NUB CIPHER KEY (PNCK) 327
PNK 325
OS NUB ID (OSNID) 330
KEY GENERATOR 210
OS NUB KEY (OSNK) 335
KEY SELECTOR 220
OS NUB CIPHER KEY (OSNK) 337
OSNK 335
APPLET-1 ID (A1ID) 340
KEY GENERATOR 210
APPLET-1 KEY (A1K) 345
KEY SELECTOR 220
APPLET-1 CIPHER KEY (A1CK) 347
A1K 345
APPLET-1 SUB-PROCESS ID (A1SID) 350
KEY GENERATOR 210
APPLET-1 SUB-PROCESS KEY (A1SK) 355
KEY SELECTOR 220
APPLET-1 SUB-PROCESS CIPHER KEY (A1SCK) 357
301
FURTHER KEY GENERATOR PROCESSING

FIG. 3

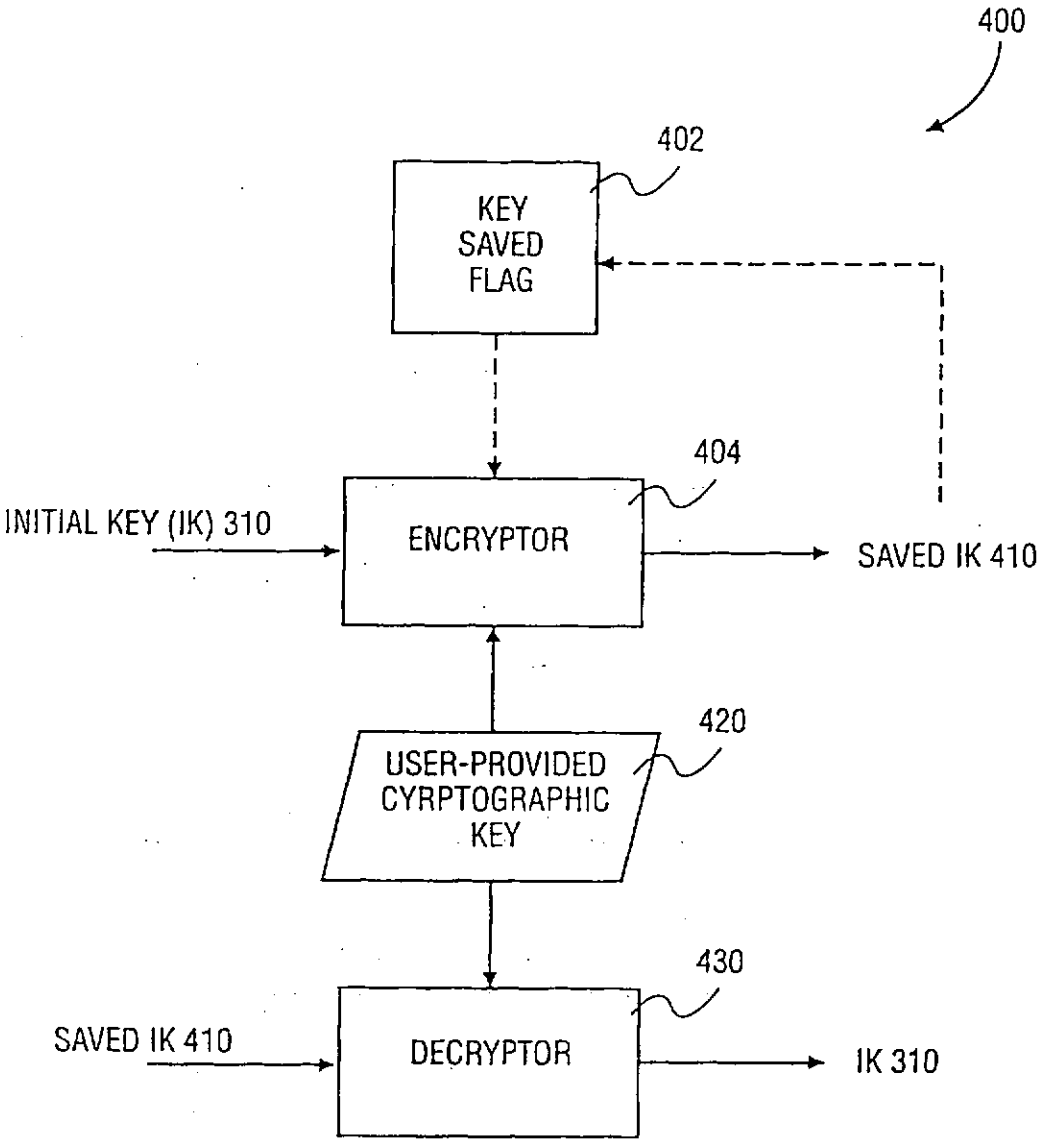

400
402
KEY SAVED FLAG
404
INITIAL KEY (IK) 310
ENCRYPTOR
SAVED IK 410
420
USER-PROVIDED CYRPTOGRAPHIC KEY
430
SAVED IK 410
DECRYPTOR
IK 310

FIG. 4

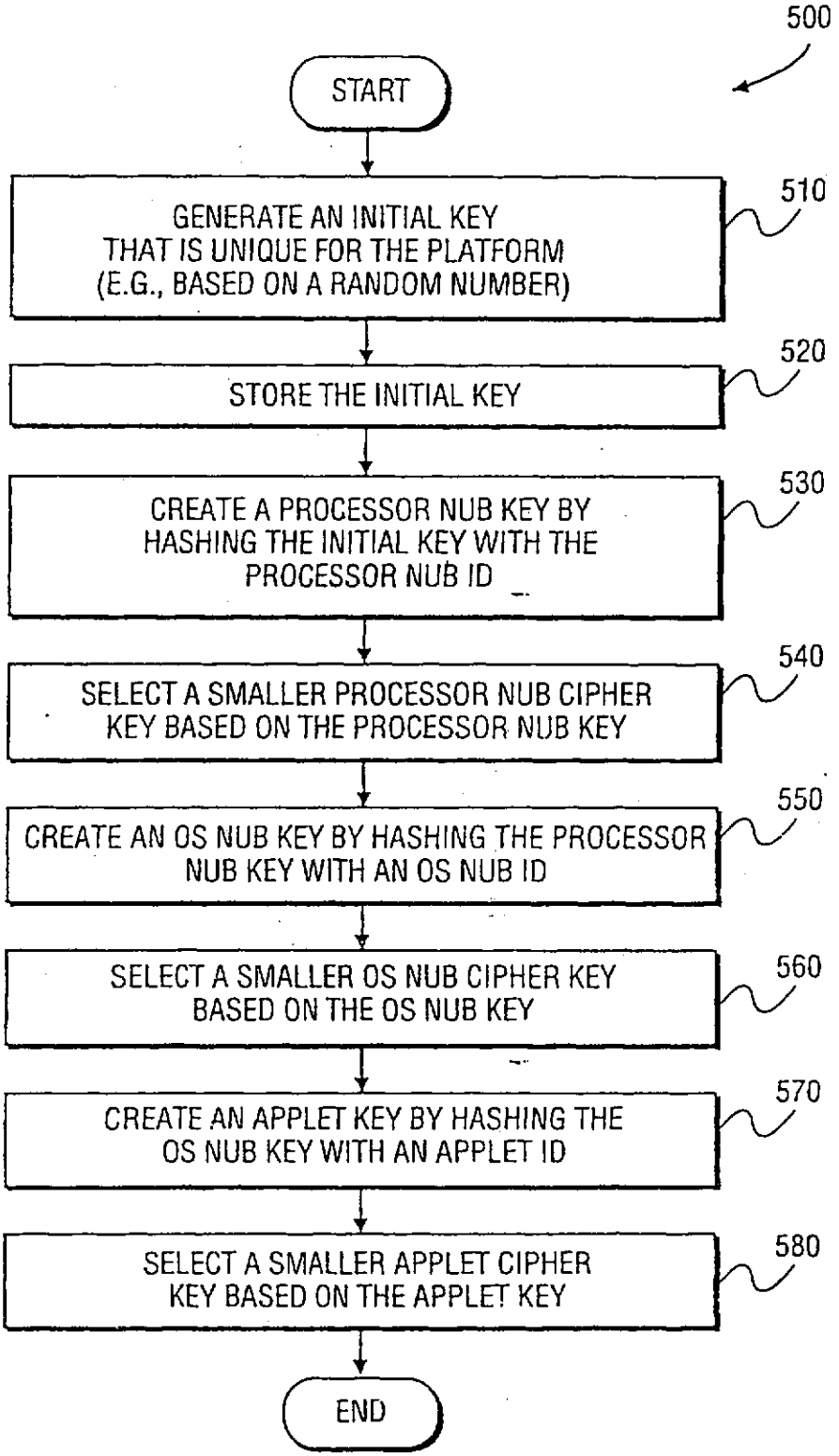

500
START
GENERATE AN INITIAL KEY THAT IS UNIQUE FOR THE PLATFORM (E.G., BASED ON A RANDOM NUMBER)
510
STORE THE INITIAL KEY
520
CREATE A PROCESSOR NUB KEY BY HASHING THE INITIAL KEY WITH THE PROCESSOR NUB ID
530
SELECT A SMALLER PROCESSOR NUB CIPHER KEY BASED ON THE PROCESSOR NUB KEY
540
CREATE AN OS NUB KEY BY HASHING THE PROCESSOR NUB KEY WITH AN OS NUB ID
550
SELECT A SMALLER OS NUB CIPHER KEY BASED ON THE OS NUB KEY
560
CREATE AN APPLET KEY BY HASHING THE OS NUB KEY WITH AN APPLET ID
570
SELECT A SMALLER APPLET CIPHER KEY BASED ON THE APPLET KEY
580
END

FIG. 5