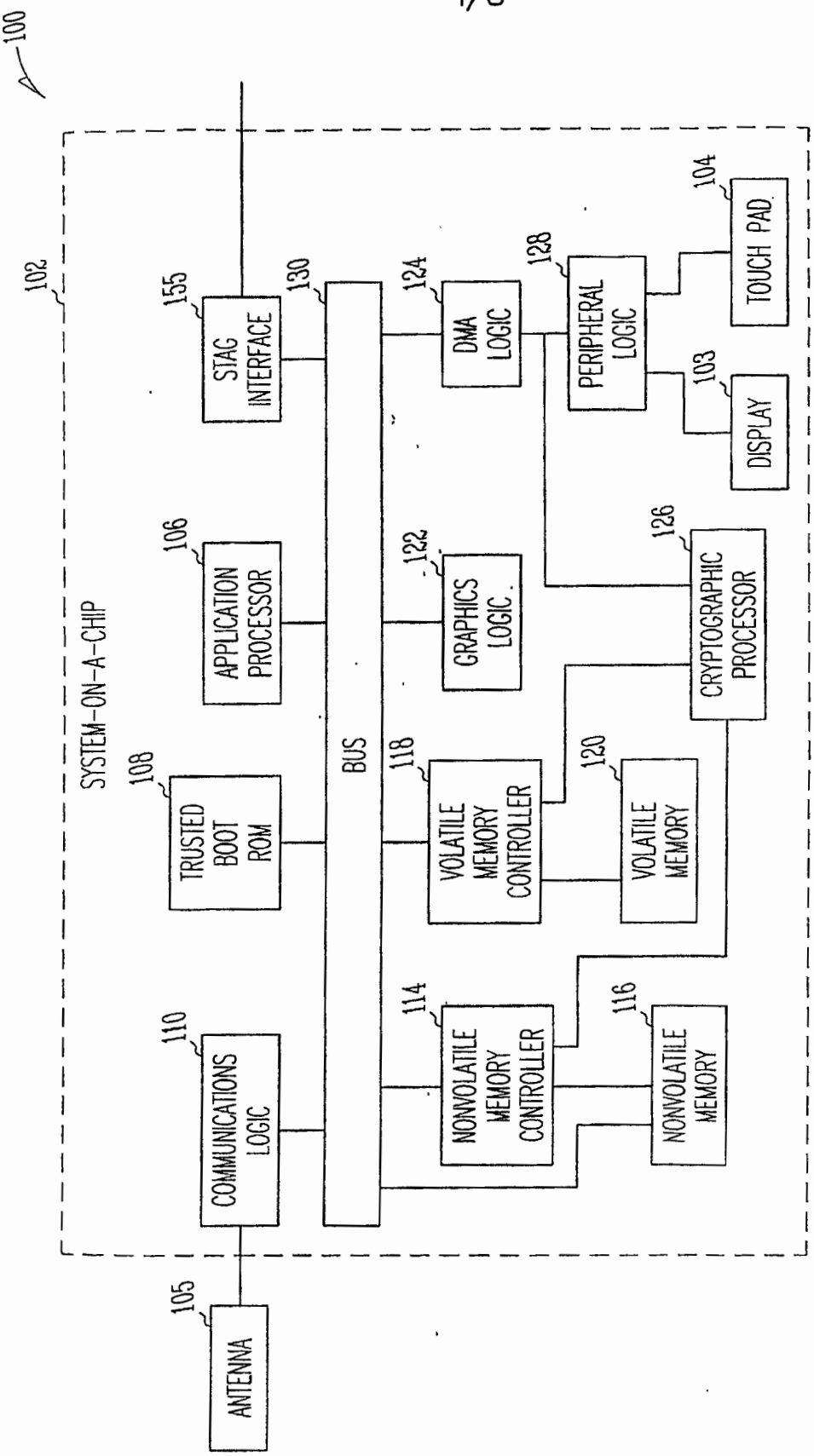

100
102
SYSTEM-ON-A-CHIP
105
ANTENNA
110
COMMUNICATIONS LOGIC
108
TRUSTED BOOT ROM
106
APPLICATION PROCESSOR
155
STAG INTERFACE
130
BUS
114
NONVOLATILE MEMORY CONTROLLER
118
VOLATILE MEMORY CONTROLLER
122
GRAPHICS LOGIC
124
DMA LOGIC
116
NONVOLATILE MEMORY
120
VOLATILE MEMORY
126
CRYPTOGRAPHIC PROCESSOR
128
PERIPHERAL LOGIC
103
DISPLAY
104
TOUCH PAD

Fig. 1

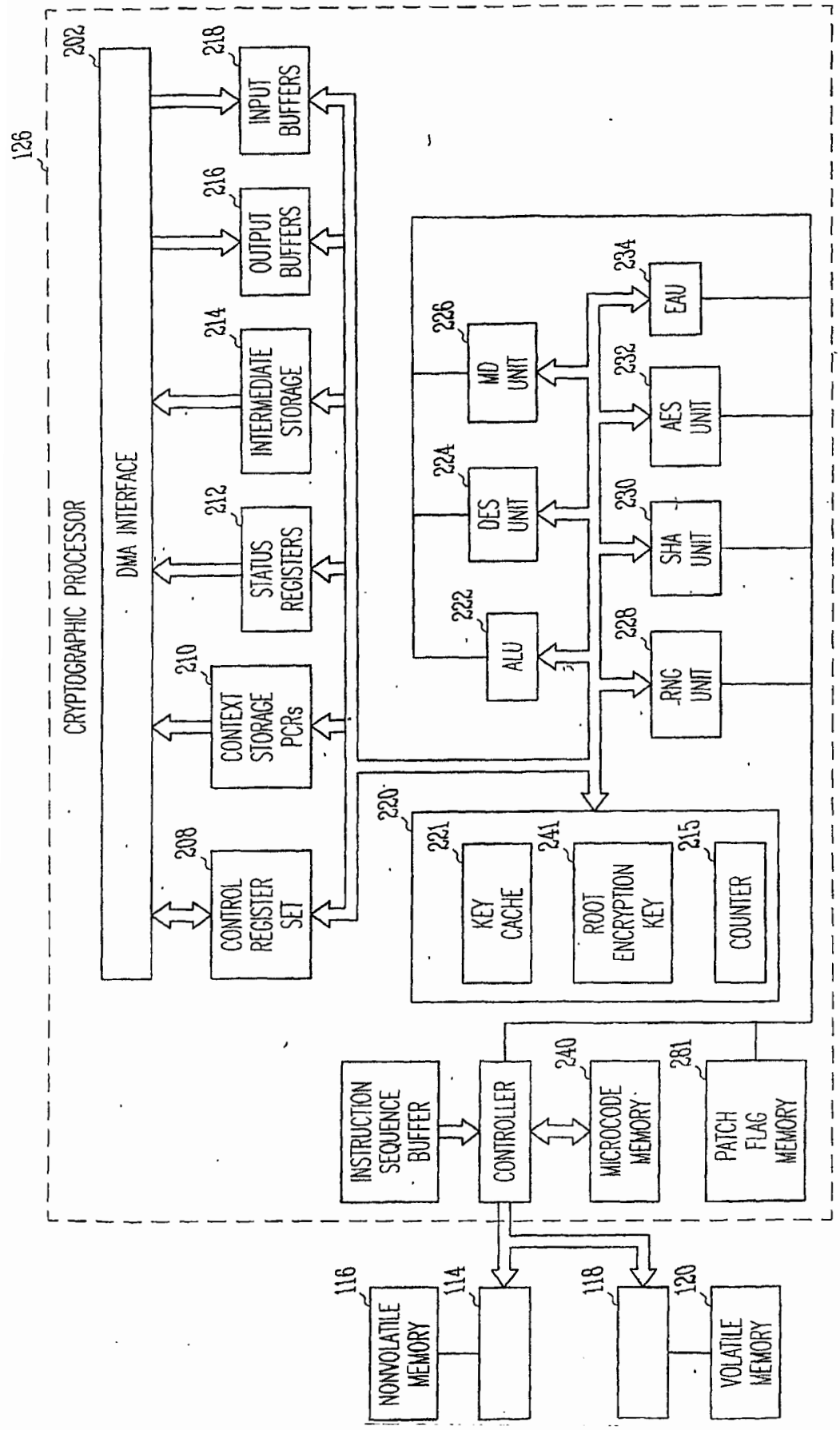

126
CRYPTOGRAPHIC PROCESSOR
202
DMA INTERFACE
218
INPUT BUFFERS
216
OUTPUT BUFFERS
214
INTERMEDIATE STORAGE
212
STATUS REGISTERS
210
CONTEXT STORAGE PCRs
208
CONTROL REGISTER SET
220
221
KEY CACHE
241
ROOT ENCRYPTION KEY
215
COUNTER
222
ALU
224
DES UNIT
226
MD UNIT
228
RNG UNIT
230
SHA UNIT
232
AES UNIT
234
EAU
INSTRUCTION SEQUENCE BUFFER
CONTROLLER
240
MICROCODE MEMORY
281
PATCH FLAG MEMORY
116
NONVOLATILE MEMORY
114
118
120
VOLATILE MEMORY

Fig. 2

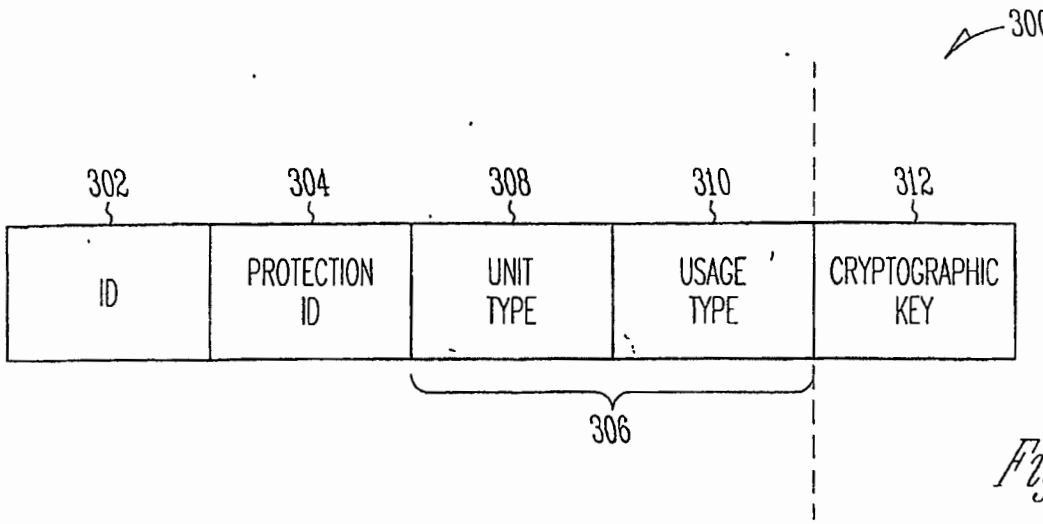

300
302
304
308
310
312
ID
PROTECTION ID
UNIT TYPE
USAGE TYPE
CRYPTOGRAPHIC KEY
306

Fig. 3

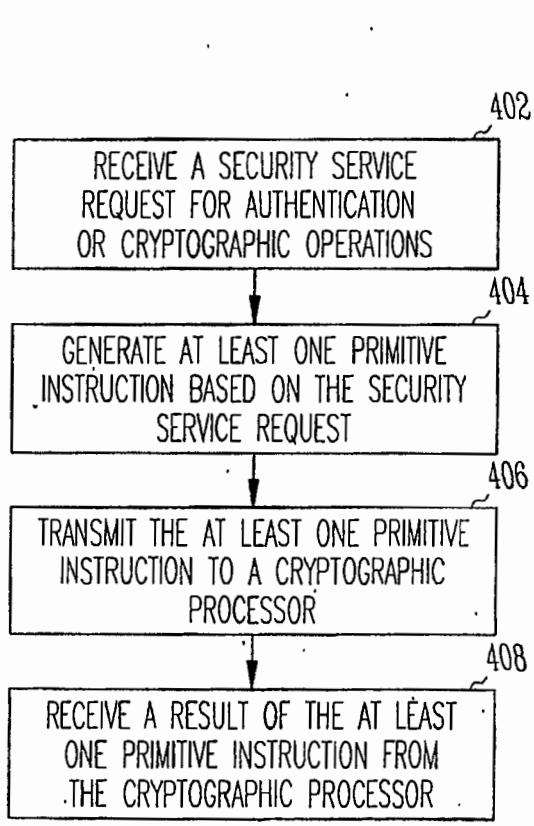

400
402
RECEIVE A SECURITY SERVICE REQUEST FOR AUTHENTICATION OR CRYPTOGRAPHIC OPERATIONS
404
GENERATE AT LEAST ONE PRIMITIVE INSTRUCTION BASED ON THE SECURITY SERVICE REQUEST
406
TRANSMIT THE AT LEAST ONE PRIMITIVE INSTRUCTION TO A CRYPTOGRAPHIC PROCESSOR
408
RECEIVE A RESULT OF THE AT LEAST ONE PRIMITIVE INSTRUCTION FROM THE CRYPTOGRAPHIC PROCESSOR

Fig. 4

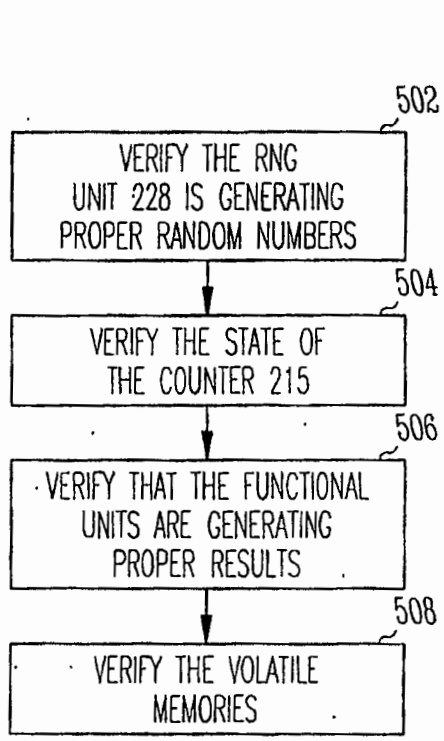

500
502
VERIFY THE RNG UNIT 228 IS GENERATING PROPER RANDOM NUMBERS
504
VERIFY THE STATE OF THE COUNTER 215
506
VERIFY THAT THE FUNCTIONAL UNITS ARE GENERATING PROPER RESULTS
508
VERIFY THE VOLATILE MEMORIES

Fig. 5

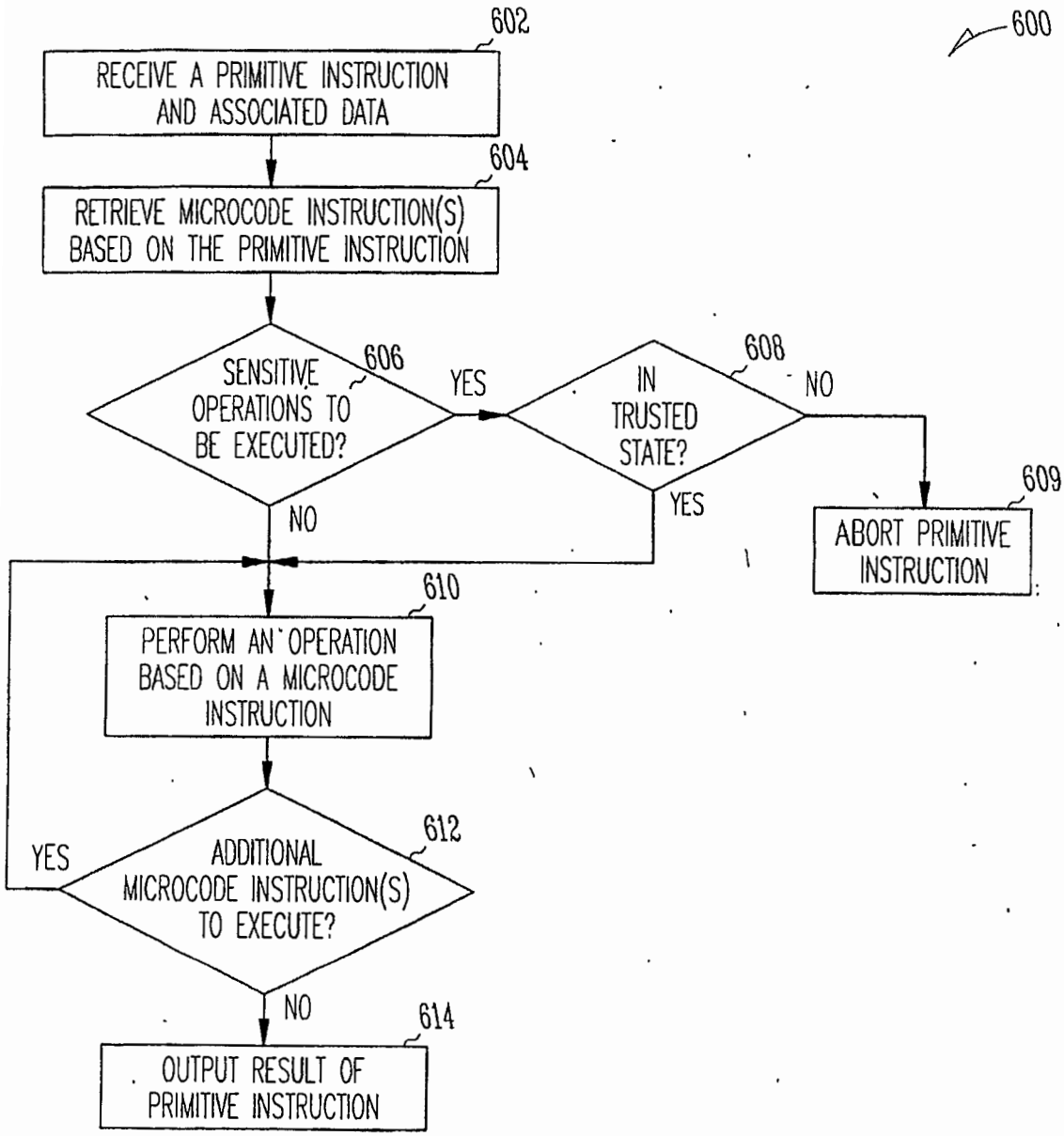

600
602
RECEIVE A PRIMITIVE INSTRUCTION AND ASSOCIATED DATA
604
RETRIEVE MICROCODE INSTRUCTION(S) BASED ON THE PRIMITIVE INSTRUCTION
606
SENSITIVE OPERATIONS TO BE EXECUTED?
YES
NO
608
IN TRUSTED STATE?
NO
YES
609
ABORT PRIMITIVE INSTRUCTION
610
PERFORM AN OPERATION BASED ON A MICROCODE INSTRUCTION
612
ADDITIONAL MICROCODE INSTRUCTION(S) TO EXECUTE?
YES
NO
614
OUTPUT RESULT OF PRIMITIVE INSTRUCTION

Fig. 6A

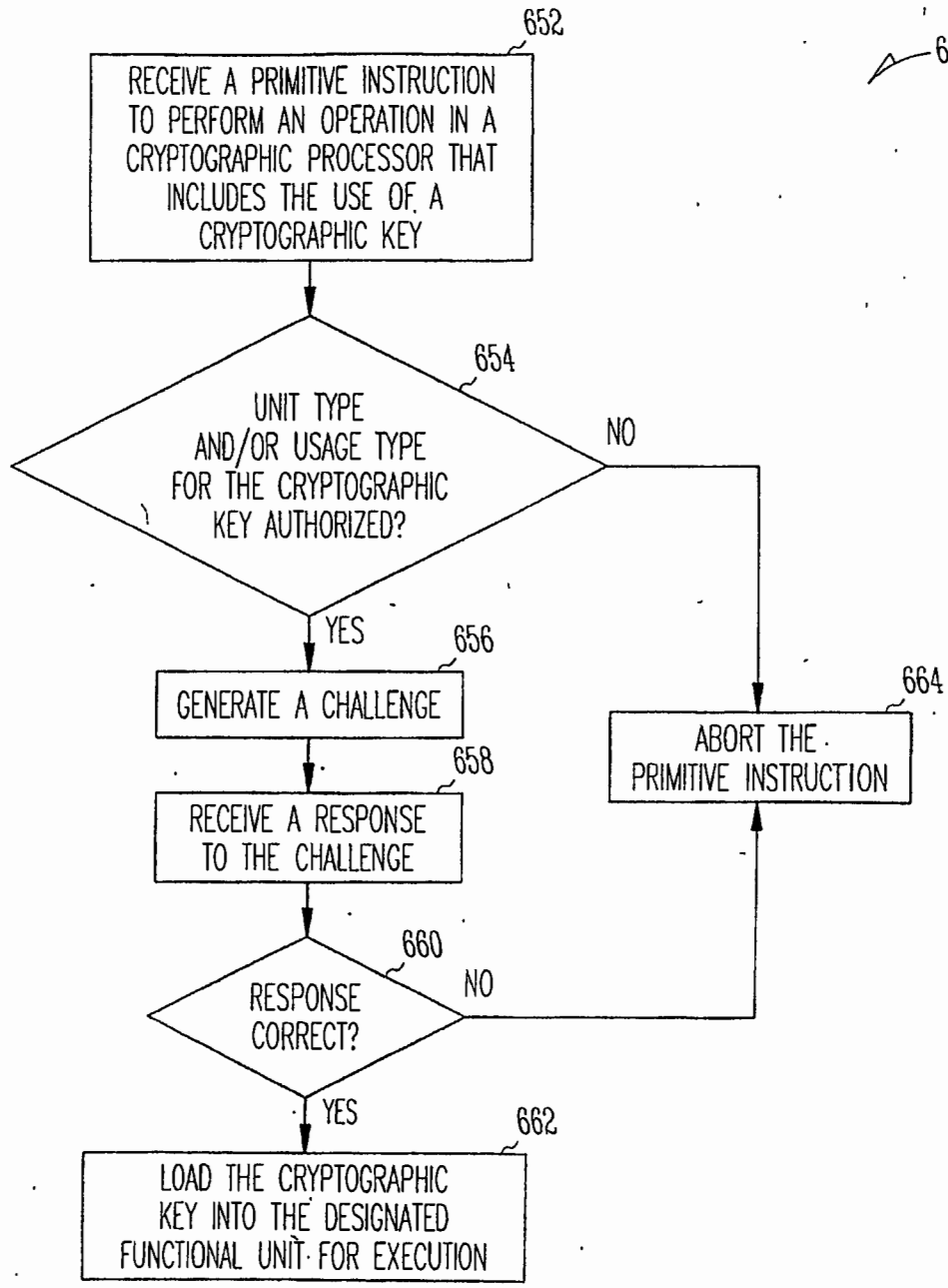

650
652
RECEIVE A PRIMITIVE INSTRUCTION TO PERFORM AN OPERATION IN A CRYPTOGRAPHIC PROCESSOR THAT INCLUDES THE USE OF A CRYPTOGRAPHIC KEY
654
UNIT TYPE AND/OR USAGE TYPE FOR THE CRYPTOGRAPHIC KEY AUTHORIZED?
NO
YES
656
GENERATE A CHALLENGE
658
RECEIVE A RESPONSE TO THE CHALLENGE
660
RESPONSE CORRECT?
NO
YES
662
LOAD THE CRYPTOGRAPHIC KEY INTO THE DESIGNATED FUNCTIONAL UNIT FOR EXECUTION
664
ABORT THE PRIMITIVE INSTRUCTION

Fig. 6B

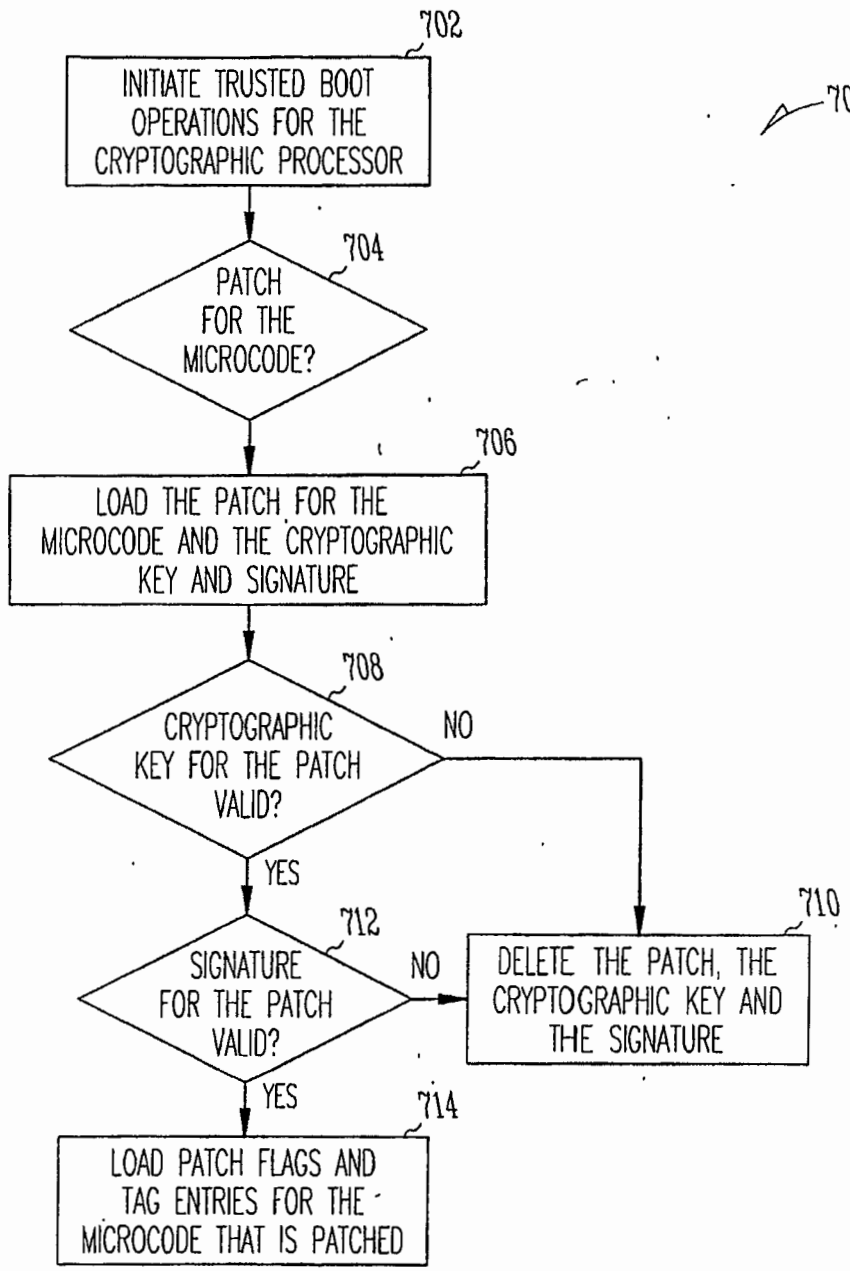

700
702
INITIATE TRUSTED BOOT OPERATIONS FOR THE CRYPTOGRAPHIC PROCESSOR
704
PATCH FOR THE MICROCODE?
706
LOAD THE PATCH FOR THE MICROCODE AND THE CRYPTOGRAPHIC KEY AND SIGNATURE
708
CRYPTOGRAPHIC KEY FOR THE PATCH VALID?
NO
YES
710
DELETE THE PATCH, THE CRYPTOGRAPHIC KEY AND THE SIGNATURE
712
SIGNATURE FOR THE PATCH VALID?
NO
YES
714
LOAD PATCH FLAGS AND TAG ENTRIES FOR THE MICROCODE THAT IS PATCHED

Fig. 7

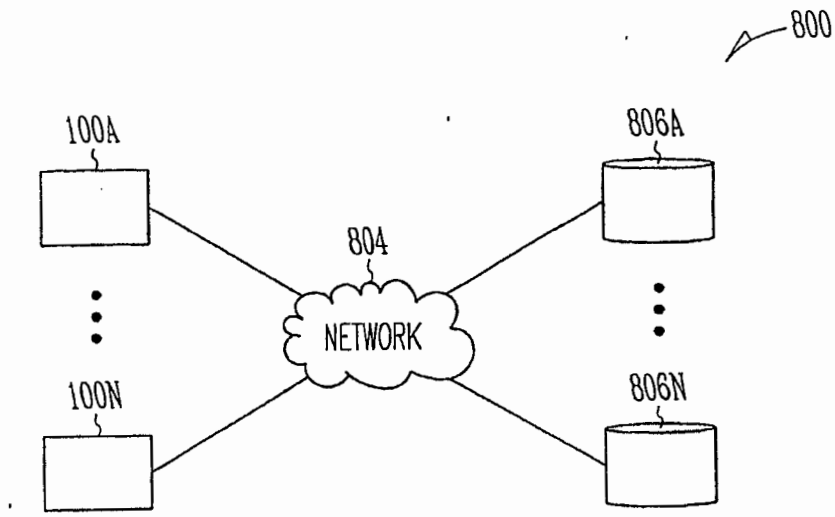


Fig. 8