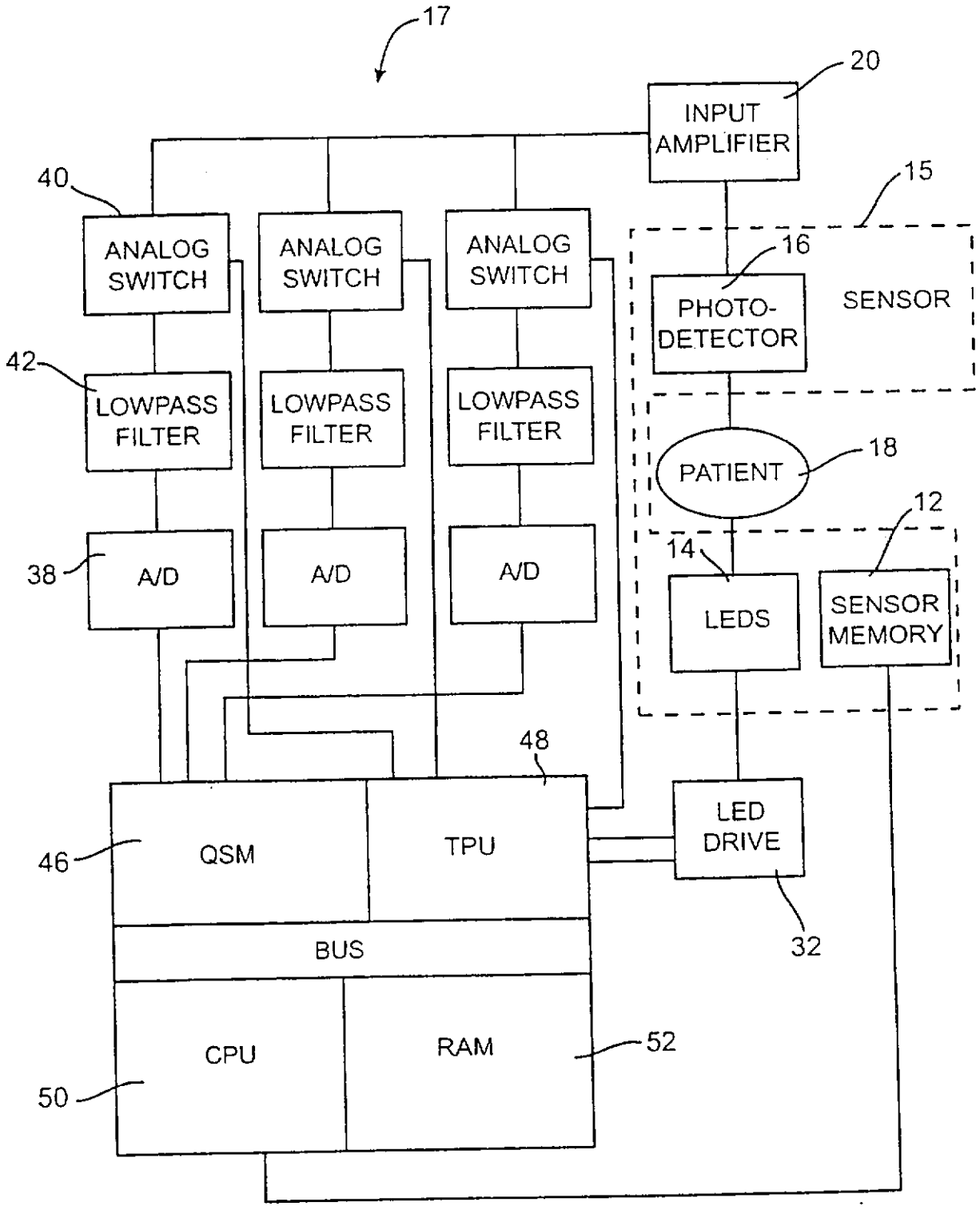

17
20
INPUT AMPLIFIER
40
15
ANALOG SWITCH
ANALOG SWITCH
ANALOG SWITCH
16
PHOTO-DETECTOR
SENSOR
42
LOWPASS FILTER
LOWPASS FILTER
LOWPASS FILTER
PATIENT
18
12
14
38
A/D
A/D
A/D
LEDS
SENSOR MEMORY
48
LED DRIVE
46
QSM
TPU
BUS
32
CPU
RAM
52
50

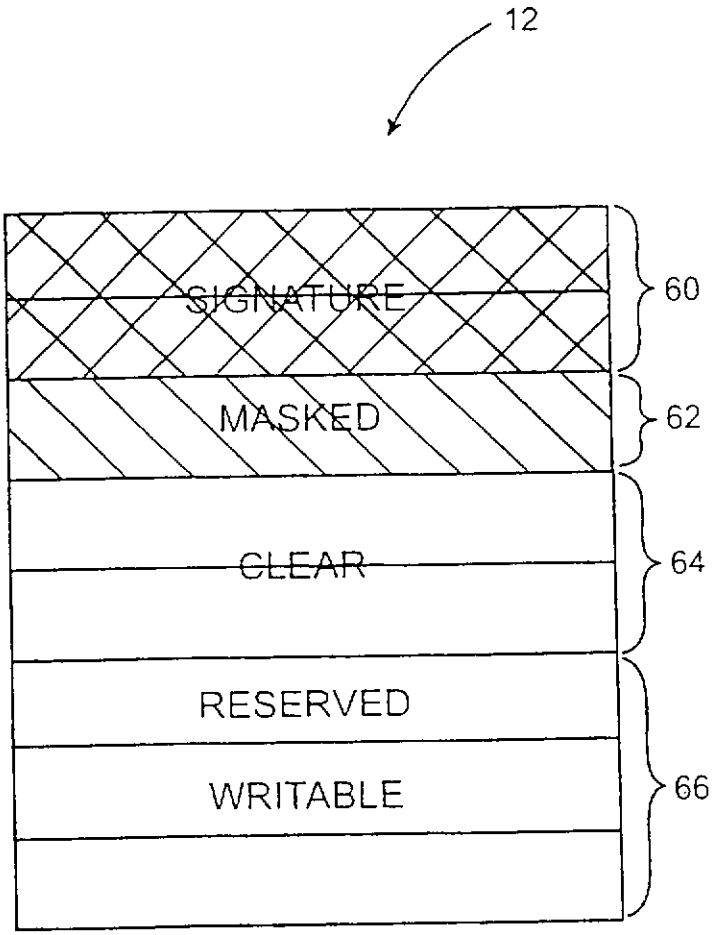


FIG. 2

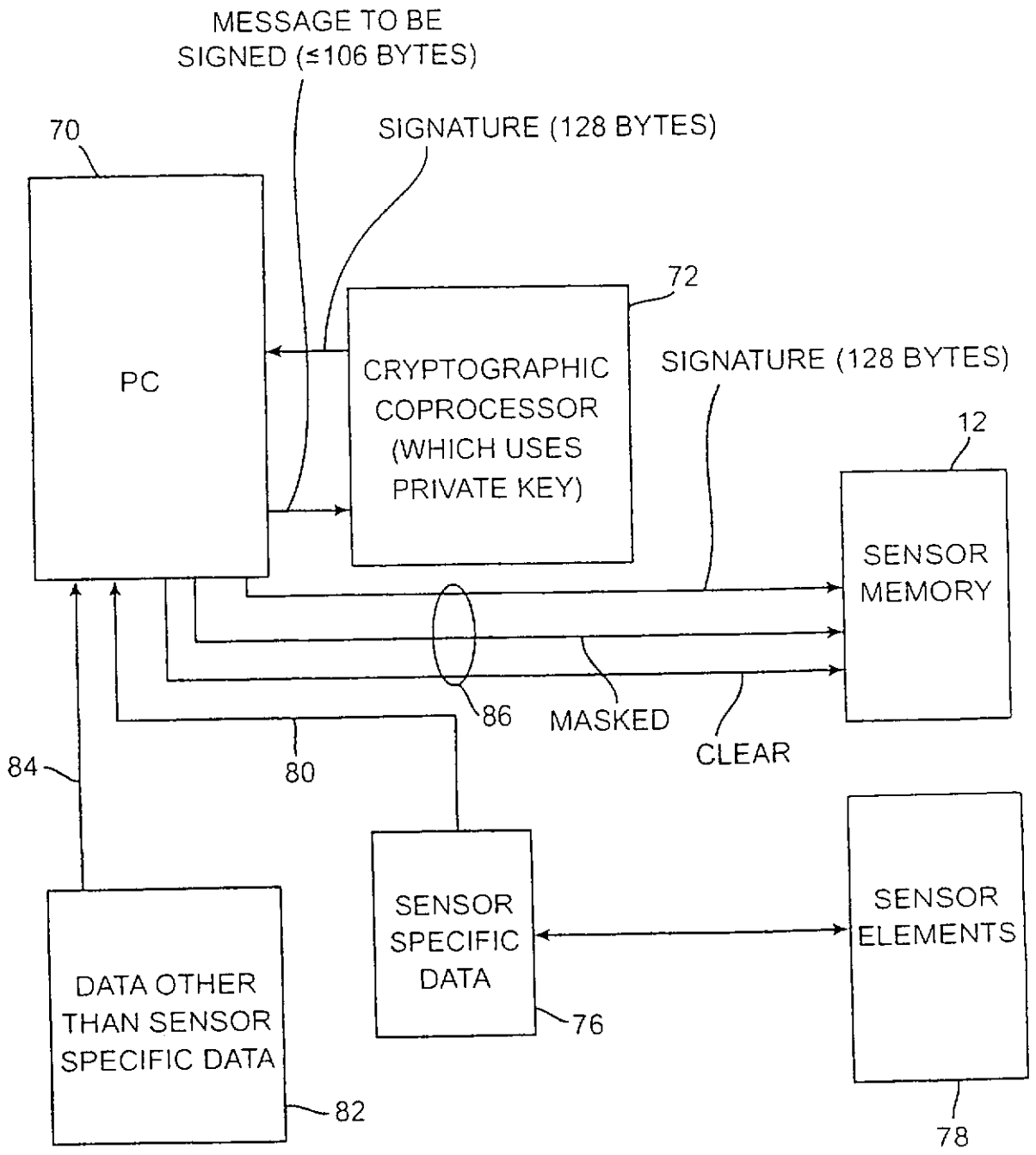

MESSAGE TO BE SIGNED (≤106 BYTES)
SIGNATURE (128 BYTES)
70
72
PC
CRYPTOGRAPHIC COPROCESSOR (WHICH USES PRIVATE KEY)
SIGNATURE (128 BYTES)
12
SENSOR MEMORY
86
MASKED
CLEAR
84
80
SENSOR SPECIFIC DATA
SENSOR ELEMENTS
DATA OTHER THAN SENSOR SPECIFIC DATA
76
82
78

FIG. 3

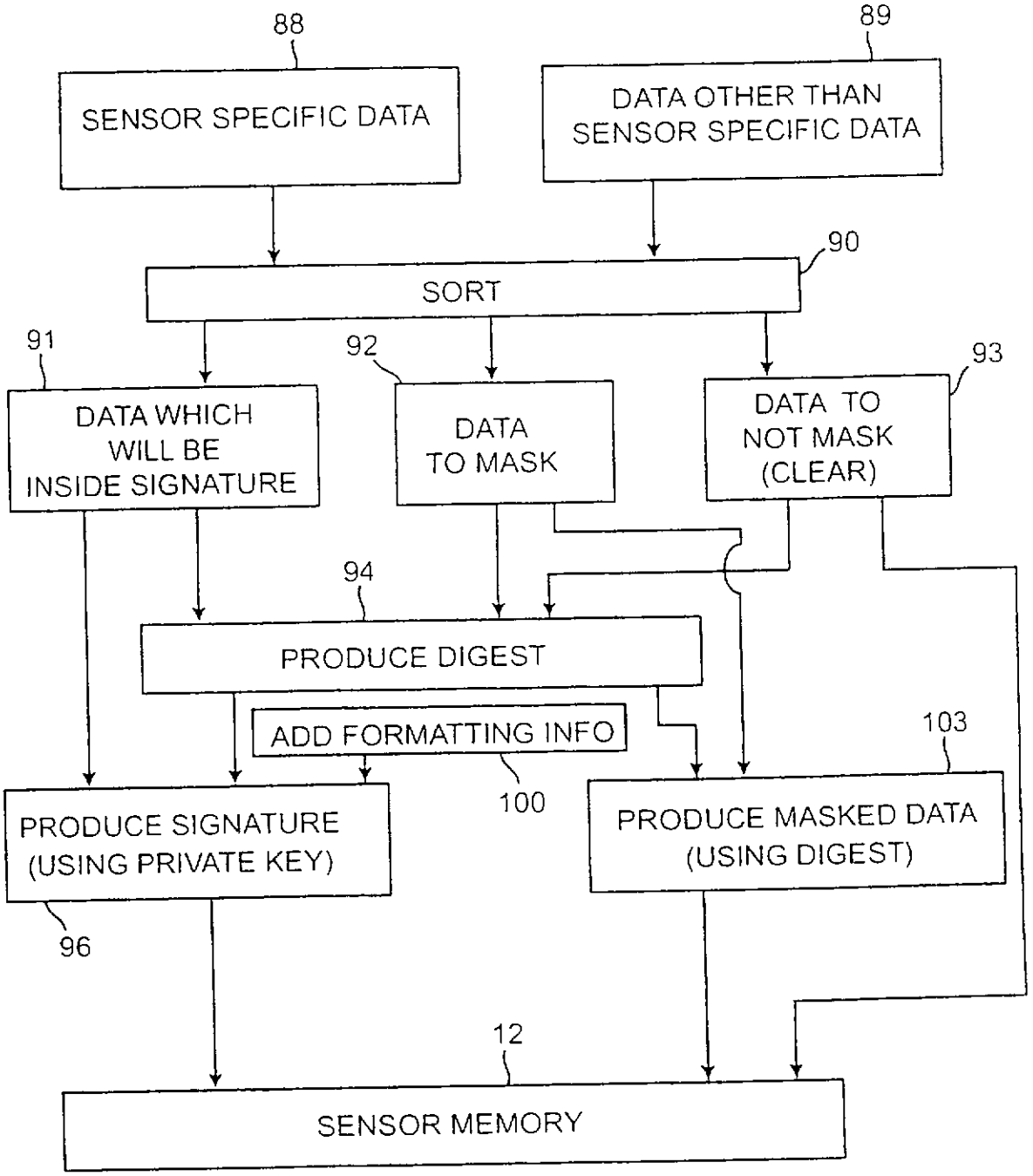

88
SENSOR SPECIFIC DATA
89
DATA OTHER THAN SENSOR SPECIFIC DATA
90
SORT
91
DATA WHICH WILL BE INSIDE SIGNATURE
92
DATA TO MASK
93
DATA TO NOT MASK (CLEAR)
94
PRODUCE DIGEST
ADD FORMATTING INFO
100
103
PRODUCE SIGNATURE (USING PRIVATE KEY)
96
PRODUCE MASKED DATA (USING DIGEST)
12
SENSOR MEMORY

FIG.4

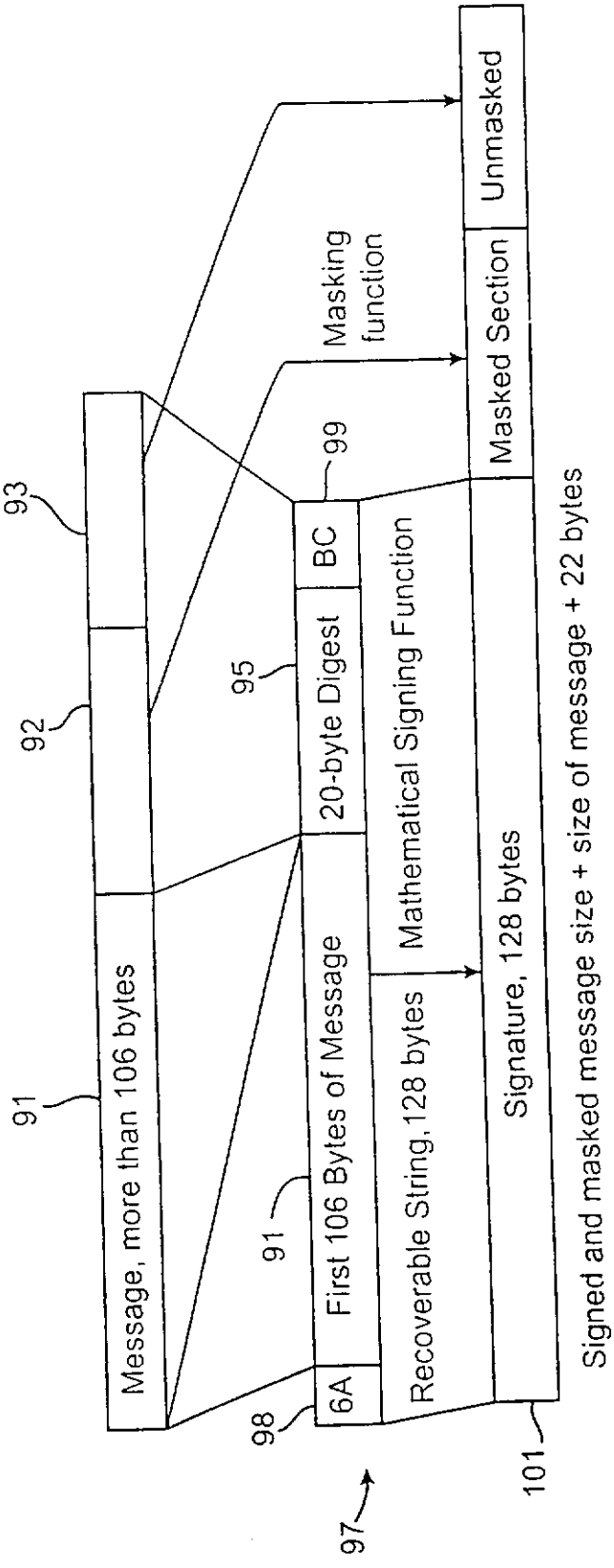

Message, more than 106 bytes
91
93
92
95
99
Masking function
Unmasked
Masked Section
BC
20-byte Digest
First 106 Bytes of Message
91
Mathematical Signing Function
6A
98
Recoverable String, 128 bytes
Signature, 128 bytes
101
97
Signed and masked message size + size of message + 22 bytes

FIG. 5

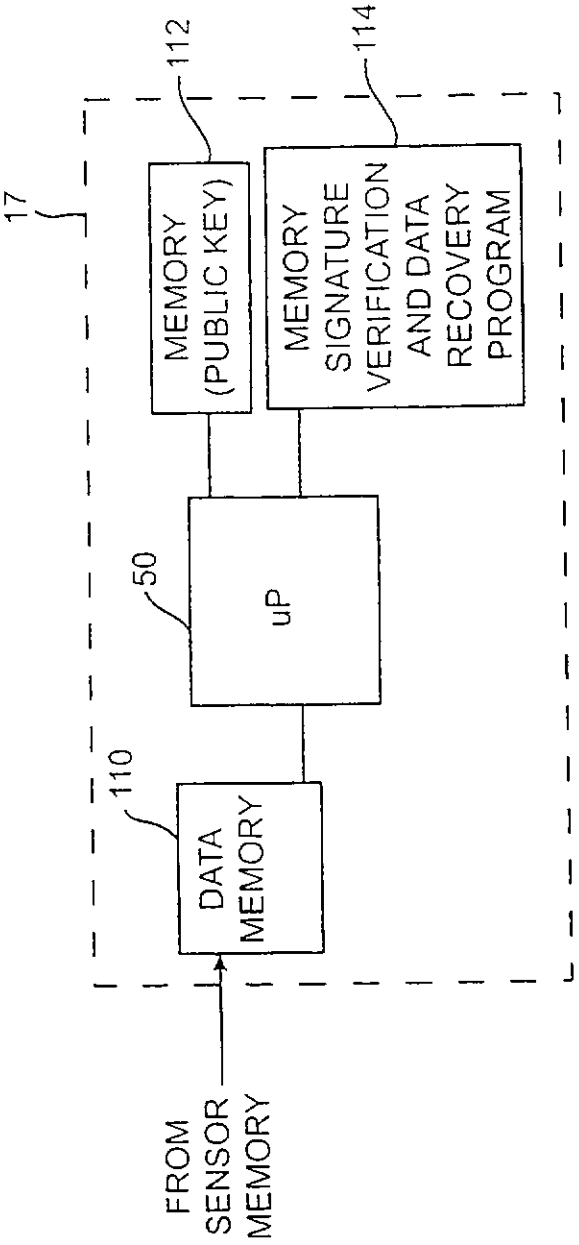

17
112
114
MEMORY (PUBLIC KEY)
MEMORY SIGNATURE VERIFICATION AND DATA RECOVERY PROGRAM
50
uP
110
DATA MEMORY
FROM SENSOR MEMORY

FIG. 6

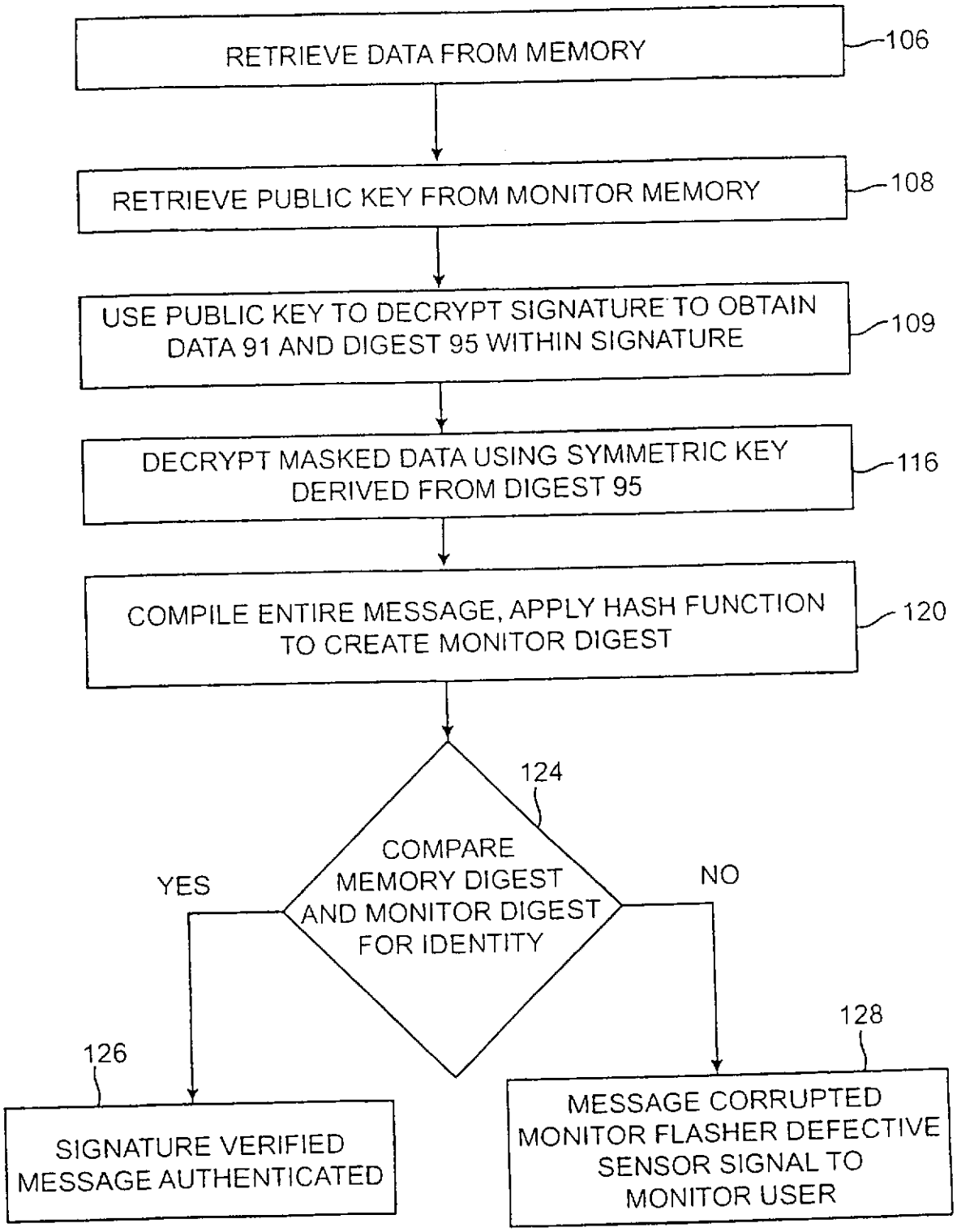

RETRIEVE DATA FROM MEMORY
106
RETRIEVE PUBLIC KEY FROM MONITOR MEMORY
108
USE PUBLIC KEY TO DECRYPT SIGNATURE TO OBTAIN DATA 91 AND DIGEST 95 WITHIN SIGNATURE
109
DECRYPT MASKED DATA USING SYMMETRIC KEY DERIVED FROM DIGEST 95
116
COMPILE ENTIRE MESSAGE, APPLY HASH FUNCTION TO CREATE MONITOR DIGEST
120
124
COMPARE MEMORY DIGEST AND MONITOR DIGEST FOR IDENTITY
YES
NO
126
SIGNATURE VERIFIED MESSAGE AUTHENTICATED
128
MESSAGE CORRUPTED MONITOR FLASHER DEFECTIVE SENSOR SIGNAL TO MONITOR USER

FIG. 7

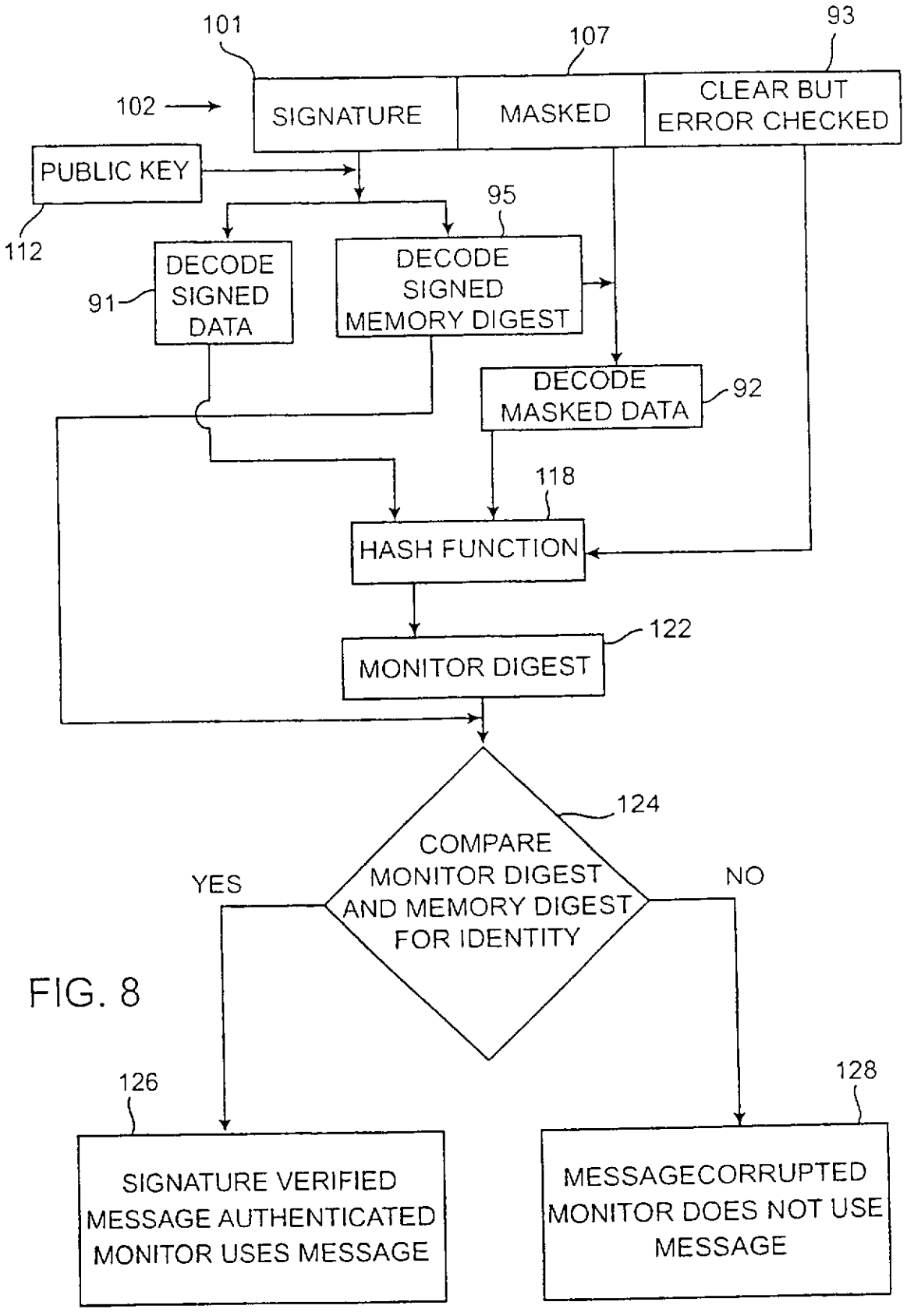

101
107
93
102
SIGNATURE
MASKED
CLEAR BUT ERROR CHECKED
PUBLIC KEY
112
95
91
DECODE SIGNED DATA
DECODE SIGNED MEMORY DIGEST
DECODE MASKED DATA
92
118
HASH FUNCTION
122
MONITOR DIGEST
124
COMPARE MONITOR DIGEST AND MEMORY DIGEST FOR IDENTITY
YES
NO
126
128
SIGNATURE VERIFIED MESSAGE AUTHENTICATED MONITOR USES MESSAGE
MESSAGECORRUPTED MONITOR DOES NOT USE MESSAGE

FIG. 8

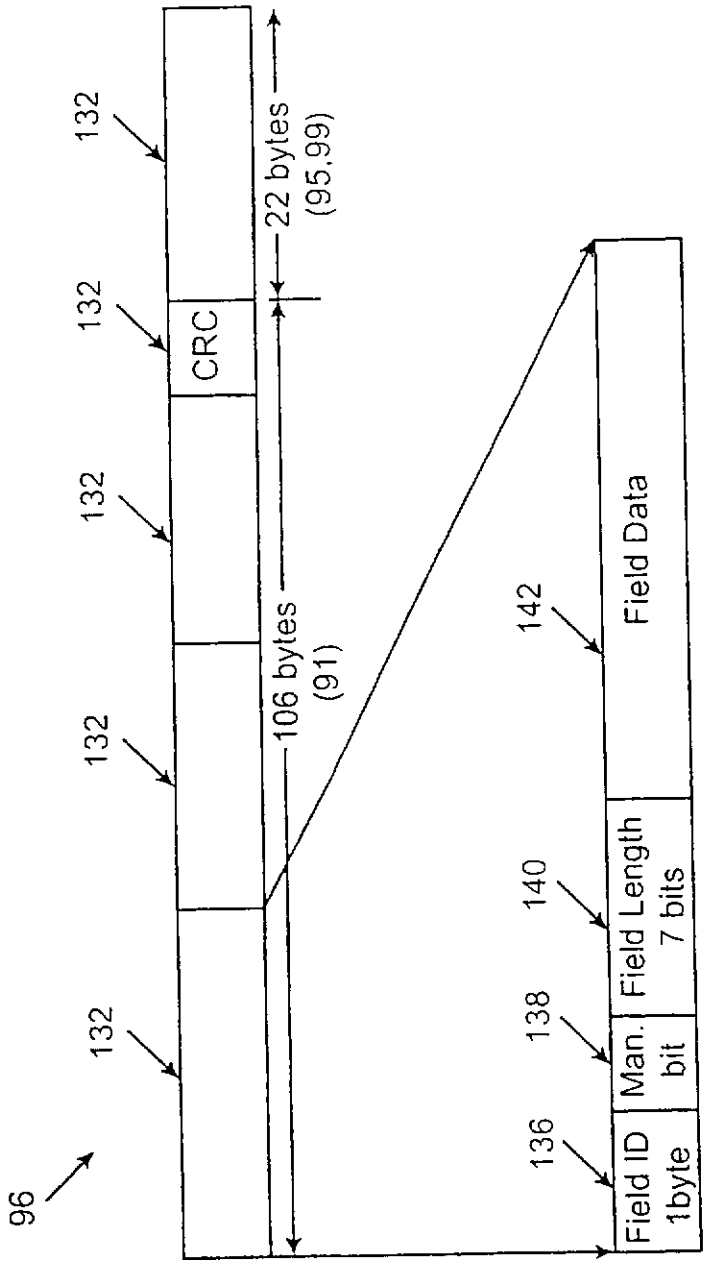

96
132
132
132
132
132
CRC
22 bytes
(95,99)
106 bytes
(91)
142
Field Data
140
Field Length
7 bits
138
Man.
bit
136
Field ID
1byte

FIG. 9

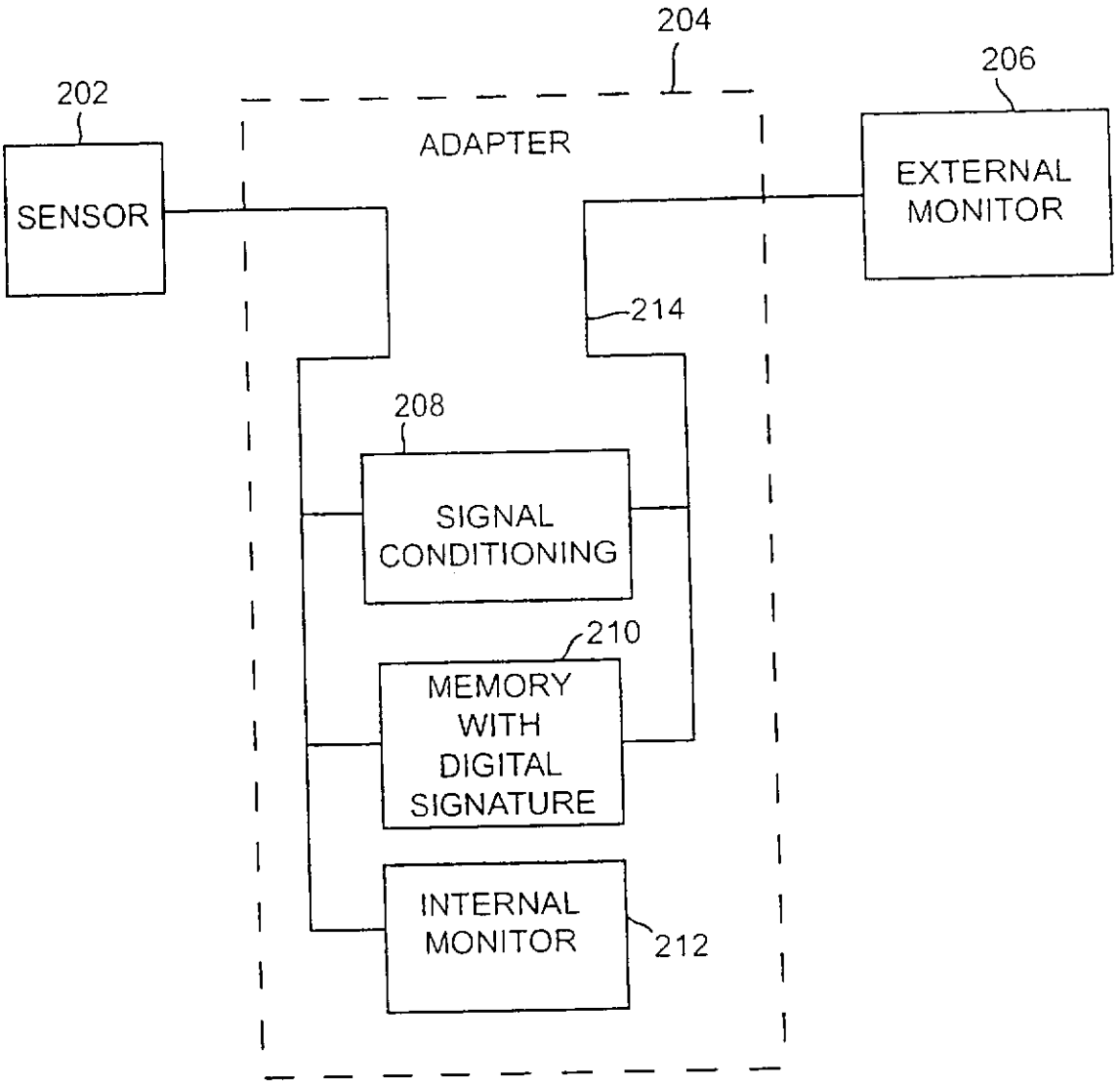

204
206
202
ADAPTER
SENSOR
EXTERNAL MONITOR
214
208
SIGNAL CONDITIONING
210
MEMORY WITH DIGITAL SIGNATURE
INTERNAL MONITOR
212

FIG. 10