(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 March 2004 (11.03.2004)

PCT

(10) International Publication Number
WO 2004/021406 A2

(51) International Patent Classification⁷: H01L

(21) International Application Number: PCT/US2003/027354

(22) International Filing Date: 29 August 2003 (29.08.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/406,758 29 August 2002 (29.08.2002) US
10/334,318 31 December 2002 (31.12.2002) US

(71) Applicant (*for all designated States except US*): **BAE SYSTEMS INFORMATION AND ELECTRONIC SYSTEMS INTEGRATION INC.** [US/US]; 65 Spit Brook Road, NHQ01-719, Nashua, NH 03061 (US).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): **LUTHI, Peter, O.** [US/US]; 31 Cathedral Circle, Nashua, NH 03063 (US).

(74) Agent: **LONG, Daniel, J.**; BAE Systems Information and Electronic Systems Int, egration Inc., 65 Spit Brook Road, NHQ01-719, Nashua, NH 03061 (US).

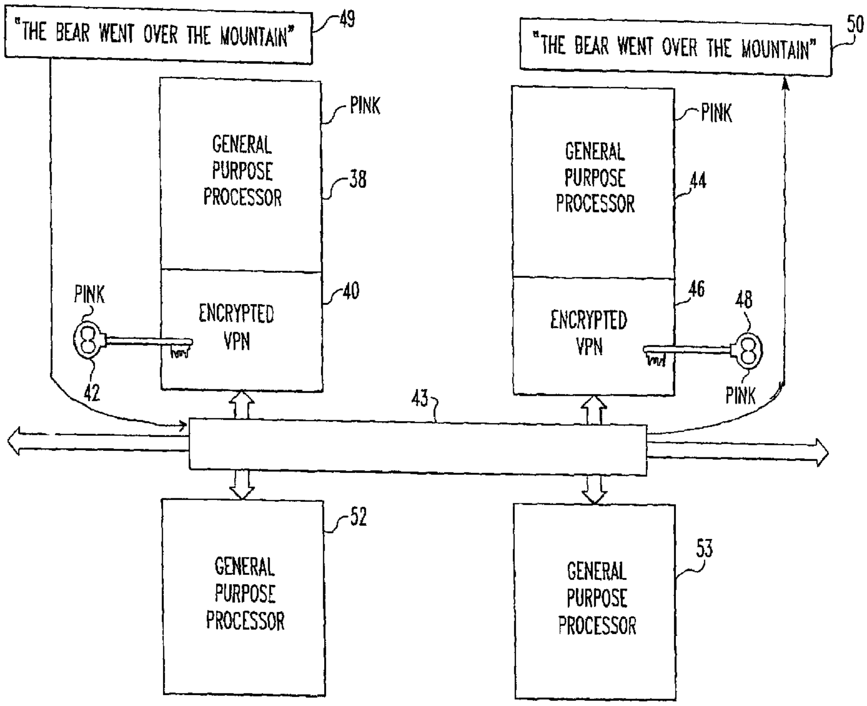
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR MULTI-LEVEL SECURITY IMPLEMENTATION


"THE BEAR WENT OVER THE MOUNTAIN"
49
"THE BEAR WENT OVER THE MOUNTAIN"
50
PINK
GENERAL PURPOSE PROCESSOR
38
PINK
GENERAL PURPOSE PROCESSOR
44
PINK
ENCRYPTED VPN
40
42
46
48
ENCRYPTED VPN
PINK
43
GENERAL PURPOSE PROCESSOR
52
53
GENERAL PURPOSE PROCESSOR

(57) Abstract: A method of operating a multi-level security system including the steps of providing a plurality of processors. At least some of said processors are equipped with a data card which permits simultaneous processing of different classification levels of information and the dynamic reallocation of processors to different classification levels.

METHOD AND APPARATUS FOR MULTI-LEVEL SECURITY IMPLEMENTATION

Cross Reference to Related Application

This application claims rights under U.S. Provisional Patent Application Serial No. 60/406,758 filed August 29, 2002

Background of the Invention

1. Field of the Invention

The present invention relates to signal and data processing, and in particular to methods and apparatus for granting privileged access to data and files by direct or indirect means. Still more particularly, the present invention relates to methods and apparatus for dynamically and automatically changing the classification level of processing elements.

2. Brief Description of Prior Developments

A multi-level security system is a system, which is capable of processing unclassified data, CONFIDENTIAL data, SECRET data, TOP SECRET data all in the same system. The conventional way that this function has been carried out is to physically separate processors. Some processors are dedicated to processing unclassified information while other processors are dedicated to processing SECRET information and still other processors are dedicated to processing TOP SECRET information. A possible problem with the above described approach is that at any instant in time the system may have much more unclassified information to process than classified information. The system may not, therefore, have enough processors to run the unclassified information, while other processors dedicated to classified information may be relatively underused.

Multi-level security has been implemented before in large networks and in systems that are custom designed but have not been implemented using commercial off the shelf processor boards in an embedded processing system.

A need therefore exists for a multi-level security system which efficiently makes use of all available computer assets. A need also exists for a multi-level security system which is capable of making use of off the shelf or other computers which may be readily available through commercial sources.

Summary of Invention

The present invention is a small data card that fits on top of the board which allows the security level of the processor to be dynamically changed by changing the keying information in the data card. This data card is called the virtual private network (VPN) card and it serves to implement the multi-level security system.

The data card which is included in the apparatus and method of the invention along with appropriate software that is an interface to a data fabric. The particular data fabric that we are pursuing currently is gigabit Ethernet although any data fabric would apply to this invention. The data fabric comes over the top of the circuit card, comes into the data card and goes into a government approved encryption device. The encryption device itself is conventional and well known to those skilled in the arë and is available from various vendors and these are approved for use on encrypting classified information. Information is decrypted when it comes on to the board and encrypted when it comes off the board. This data card is always used in sets of cards and the basic concept is that when classified information at for example, the SECRET level needs to be transferred from one board to another board at the SECRET level that goes through the data card becomes encrypted and is put on the data fabric encrypted so that it is no longer classified information. It is then transferred over to the circuit card and it is decrypted and then sent to the commercial processing board where it is processed. Only cards that have the same key can process the SECRET information. The user has another circuit card with the VPN processing data at, for example, the CONFIDENTIAL level. Any attempt to send information from a SECRET module to a CONFIDENTIAL module will not succeed. The module will have a different key and that information will not be properly decrypted so it will not be received by the CONFIDENTIAL processing module. The user or controlling software then is provided a means to change the classification level of a processing card without any physical changes. For example, if a CONFIDENTIAL card wants to or needs to be changed or reallocated to SECRET processing, the trusted system software will zeroize the circuit card, clearing all the information of it, give it the SECRET level key and now that processor, which used to process CONFIDENTIAL information, is now capable of processing SECRET information. The VPN card provides the physical red/black boundary, making it possible to use commercial boards for classified processing, the unclassified information (black side) being the data fabric and the classified information (red side) being on the circuit card is on the data card. The user does not have to have any red/black boundaries on the commercial circuit card. The VPN card satisfies the requirements imposed by the government to implement the red/black boundary, some of those include tempest and encryption and these are all concentrated on to the small data card so that the user does not have to design the entire circuit card to the government specifications.

For purpose of this disclosure, the term "red" refers to all types of classified information generally and the term "black" refers to unclassified information. As used hereafter "pink", "purple" and "orange" are classes of "red"

Brief Description of the Drawings

The present invention is further described with reference to the accompanying drawings in which:

Figure 1a is a front perspective view of a commercial off the shelf (COTS) processor board with a virtual private network (VPN) encryptor peripheral component interconnect mezzanine card (PMC) daughter card which comprises a preferred embodiment of the method of the present invention;

Figure 1b is a schematic diagram showing the operation of the COTS processor and VPN encryptor shown in Figure 1a;

Figure 2 is a schematic diagram showing a method by which encrypted VPN supports red/black separation on a single data fabric as is used in a preferred embodiment of the method of the present invention;

Figure 3 is a schematic diagram showing encrypted VPN support of multi-level security as is used in a preferred embodiment of the method of the present invention;

Figure 4 is a schematic diagram illustrating a method by which the Information Security (INFOSEC) module controls intra-level communications and key management as is used in a preferred embodiment of the method of the present invention;

Figure 5 is a schematic diagram illustrating encrypted VPN permitting dynamic allocation of assets to different security levels as is used in a preferred embodiment of the method of the present invention;

Figure 6 is a schematic diagram illustrating the implementing of a communications path with reconfigurable assets as is used in a preferred embodiment of the method of the present invention; and

Figure 7 is a schematic diagram illustrating the implementing of a jammer with reconfigurable assets as is used in a preferred embodiment of the method of the present invention.

Detailed Description of the Preferred Embodiment

Referring to Figure 1a, there is a COTS processor board 10 on which is affixed the VPN encryptor 12, which is a PMC daughter card that makes use of an approved INFOSEC chip. This daughter card is designed to support red/black separation and is not a COTS product. The processor board runs on the red side. The backplane 14 isolates power and simple controls and forms another red/black boundary using techniques such as filters 16 18.

The COTS processor board 20 typically includes processors and memories 22, 24, 26, and 28 which are interconnected with a data switch 30. The data switch 30 is interconnected with a VPN encryptor 32 which has a key manager function 34 and a zeroised function 36 which are explained in greater detail hereafter.

Referring to Figure 2, there is a COTS general purpose processor board (GPP) 38 with an encrypted VPN 40 having a key 42 which is interconnected by way of a bus 43 to a second general purpose processor 44 with an encrypted VPN having a key 48. This key 48 is the same as key 40; therefore, data 49 contained in general purpose processor 38 is encrypted by the VPN card 40, transferred over the data fabric of bus 43, is decrypted by the VPN card 46 and received by general purpose processor 44. The information 49 exchanged between GPP 38 and GPP 44 (and received at GPP 44 as information 50) cannot be intercepted by unclassified GPP 52 or GPP 53 because the data is encrypted as it is transferred over the data fabric or bus 43.

Referring to Figure 3, GPP 54 with an encrypted VPN 56 and key 58 is shown. This GPP is interconnected through bus 59 to a general purpose processor 60 with an encrypted VPN 62 and key 64. Key 64 is different from key 68; therefore, data or message 66 in general purpose processor 54 is not encrypted as data message 67 in GPP 60.

Still referring to Figure 3, there are two VPN cards 56 and 62 on GPP's 54 and 60 respectively which are keyed for two different classification levels, e.g. CONFIDENTIAL designated pink and SECRET designated purple and there is a message 66 which gets encrypted and gets put on the bus 59, and is sent to the GPP 60 via the VPN 62. This board tries to decrypt the message 66 with the wrong key, so that garbled information is received so it does not get the final message. All the information that goes across the data fabric is unclassified information which is either purely unclassified or classified information that has been encrypted and so unclassified GPPs 68 and 69, cannot access any classified information. Accordingly, computers at the SECRET level can talk to each other. Computers at the TOP SECRET level can talk to each other. Computers at the unclassified level can talk to each other. Computers of different classification cannot directly communicate. If, for example, a SECRET computer tries to talk to a CONFIDENTIAL computer the information cannot go through. The only way the user can do that is to go through a government certified device that allows that type of information flow which is called the guard function. The guard function examines the content of messages, rate of messages, and other message parameters and determined, by a series of pre-defined security policies, whether the information should be permitted to cross between classification levels. So each type of GPP has a key at its own classification level and so if it is desired to change these from, for example, from TOP SECRET to SECRET, first the trusted software of this implementation deletes the keys and that makes the two boards unclassified. The key management function of this implementation then provides new keys. For example, if the user wants to change to the CONFIDENTIAL level he can have four boards that can run at the CONFIDENTIAL level. The user can also use the same boards to process unclassified information by zero zing the key. Now the user can run the GPP at the bypass mode and can run unclassified information on it.

Referring to Figure 4, there is an INFOSEC module with a VPN card 64 with keys 66, 68, and 70. There are also COTS general-purpose processors (GPP) with VPN cards 72, 74, 76, 78, 80, and 82. There are also unclassified GPP=s 84, 86, 88, and 90. In this arrangement the INFOSEC module 64 controls intra-level communications and key management. It is understood from the previous discussions that information can be passed over the data fabric or bus 91 between like classification levels, but not between different classification levels. It will be understood from Figure 4 that information can be transferred between different classification levels only by passing the information through the trusted guard function on the INFOSEC module. It can be passed between the unclassified GPP's 84, 86, 88 and 90. The information can also be passed directly between the boards at one classification level 80, 82 which are the same classification level. The information can be passed between boards at a different classification level 76 and 78 and all of these information transfers can occur at the same time. If a board at one classification level at GPP 80 attempts to send information to another GPP allocated to a different classification level at GPP 74 that information cannot be passed as was described in connection with Figure 3. Instead, that information must got through an information security module which contains the keys for all classification levels and includes a trusted guard function which implements the security policies for sending information between different classification levels. If COTS GPP 82 has information that needs to be sent to COTS GPP 72 which is operating at a different classification level it is first sent to the INFOSEC module. The data is encrypted by the VPN at GPP 82, goes across the data fabric, is decrypted by the VPN with the orange key. That information and then checked by the trusted guard function. If it meets the security policies, it is re-encrypted with the pink GPP 72 and the information is then sent over the data fabric encrypted with that key, decrypted by the VPN on processor 72 and the information then can be received.

Referring to Figure 5, there is an INFOSEC module with VPN card 92 with keys 94, 96, and 98. There are also COTS GPP's with VPN cards 100, 102, 104, 106, 108, and 110 which have respectively keys 112, 114, 116, 118, 120, and 122. There are also unclassified GPP=s 124, 126, 128, and 130. In this arrangement the encrypted VPN permits dynamic allocation of assets to different security levels. It will be understood from Figure 5 that the classification level of processors can be changed by the trusted software by deleting the key in the VPM module, zeroizing the COTS processor, which means wiping out any information in the memory, and reloading it with a different key. In this way the COTS processor can dynamically change from one classification level to another without the need to effect any physical changes to the system.

Referring to Figure 6, an arrangement is shown with an antenna 132, a T/R switch 134, a tuner 136, an FPGA card 138, GPP's with VPN cards 140 and 142, which in this instance are set to perform unclassified processing, government authorized cryptographic equipment 144 implemented on the INFOSEC modules discussed earlier, and red side processing GPP with VPN card 146. There is also a user interface (I/F) with VPN card 148 as well as another GPP with VPN card 150, an exciter with VPN card 152, a PA 154, a T/R switch 156 and an antenna 158. It will be understood from Figure 6 and figure 7 generally, that one possible application of the invention in which the user has a multi-mission system which is to be capable of simultaneously performing communications, signal intelligence (SIGINT) and jamming. Conventionally these three capabilities are implemented by three totally separate systems and the security approach used today would prohibit those functions from being implemented simultaneously in the same system. It will be understood that the method and apparatus of this invention can allow information to be separated and allows the two functions to occur simultaneously. The solid line shows the receive communications path from the antenna 158 being received by the tuner 136 implementing a modem in the FPGA card 138 in the black side general purpose processor 140. Additional black side processing occurring on the general purpose processor 142. Information then goes to the crypto device 144 which may be the INFOSEC module 144 described in connection with Figure 6. The information then gets the key change as described on Figure 4 and is sent to the classified processing on the general purpose processor 146 is then sent out to the user to receive the data through the user interface 148. The information to be transmitted from the user out the radio communication functions is received by the user interface 148 as SECRET level data and is sent over to a GPP the same classification level where the red side processing of the radio occurs. It is then sent over the data fabric to the crypto logical device located on the information security module 144 where the data is encrypted for transmission. From where it goes to the transmit black side processing at GPP 142 it then goes to a GPP 150 also on the black side where the transmit half of the modem is prepared, over the VPN in this case in the bypass mode because data is being transferred from a black processor to a black processor, out to the excitor 152 and the information is sent through the power amplifier 154 out to the transmit receive (TR) switch 156 and transmitted out the antenna 158. In this way, the user can implement a secure radio using the invention as a reconfigurable software programmable radio.

Referring to Figure 7, an arrangement is shown in which there is a antenna 160, a tuner 162, an FPGA card 166, a GPP with VPN card 166 for signal detection, a GPP with VPN card 168 for signal identification, a guard 170 with VPN card 170, and a GPP with VPN card 172. There is also a User I/F with VPN card 174, a GPP with VPN card 176, an exciter with VPN card 178, a PA 180 and an antenna 182. It will be understood from

Figure 7 that it is shown that the same hardware configuration used for communications in Figure 6 can be used simultaneously for signals intelligence (SIGINT) simultaneously with communications signal jamming. For SIGINT the target signal is received by the antenna 160 and processed by the tuner 162 and then sent to the FPGA card 164 which implements a fast transform FFT. That information is then passed over the switch data fabric to the general purpose processor 166 which implements the signal detection function. The information is then passed to provide some additional classified processing. In order to accomplish this processing the information is sent to the guard function on the INFOSEC module 170 where it allows information to be passed in an unrestricted way from the unclassified side of the system to the classified side of the system but has a means to insure that no information can accidentally be leaked back in the other direction. The information is then encrypted with the classified level key on the VPN card mounted on the INFOSEC module 170 and sent over to the general purpose processor 168 which is running at the classified level. The processor then does a signal identification. That information is further processed and sent to another computer operating at the same classification level 172 that performs additional processing such as target identification. That information then is reported to the user, operating at the classified level and so it is sent across the VPN across the user interface and out to the user. In this way the user can get the SIGINT information that was processed by the system.

Using the same hardware and running at the same time, communication signal jamming may be accomplished. A command comes from the user to perform the jamming through the user interface 174 this is a classified level command that is then sent over the VPN to the general-purpose processor 176. That information is then sent to the exciter 178 where the RF signal is generated and it is sent to the power amplifier 180 and out the antenna 182.

It will be appreciated that a method and apparatus for operating a multi-level security system has been described which efficiently makes use of all available computer assets. It will also be appreciated that this method and apparatus can make use of off the shelf or other computers, which may be available through commercial sources.

While the present invention has been described in connection with the preferred embodiments of the various figures, it is to be understood that other similar embodiments may be used or modifications and additions may be made to the described embodiment for performing the same function of the present invention without deviating therefrom. Therefore, the present invention should not be limited to any single embodiment, but rather construed in breadth and scope in accordance with the recitation of the appended claims.

Claims

What is claimed is:

1. A method of operating a multi-level security system comprising the steps of providing a plurality of processors for processing different classification level of information; simultaneously processing said different classifications levels of information; and reallocating at least one of said processors from processing one of said classification levels of information to another of said classification levels of information.

2. The method of claim 1 wherein a data card is provided for allowing the simultaneous processing of said different classification levels of information and reallocating at least one of said processors from processing one classification level of information to another.

3. The method of claim 2 wherein the data card is an encryption means.

4. The method of claim 3 wherein the data card includes an information security means.

5. The method of claim 4 wherein the data card is a daughter card.

6. The method of claim 1 wherein the processors are dynamically reallocated.

7. The method of claim 1 wherein the classification levels are TOP SECRET, SECRET and CONFIDENTIAL.

8. A multi-level security system for processing a plurality of different classification

levels of information, comprising:

a plurality of processors for collectively processing information simultaneously processing information from two or more of said plurality of different classification levels of information; and

means for reallocating at least one of said different classification levels of information to another one of said classification levels of information.

9. The system of claim 8 wherein the means for reallocating at least one of said different classification levels is a data card.

10. The system of claim 9 wherein that data card is an encryption means.

11. The system of claim 10 wherein the data cards includes an information security means.

12. The system of claim 11 wherein the data card is a daughter card.

13. The system of claim 8 wherein the means of reallocating at least one of the processors dynamically reallocates said processors.

14. The system of claim 8 wherein the classification levels are TOP SECRET, SECRET and CONFIDENTIAL.

15. A multi-level security system for processing a plurality of different classification levels of information, comprising:

a plurality of processors for collectively processing information simultaneously processing information from two or more of said plurality of different classification levels of information; and a data card for reallocating at least one of said different classification levels of information to another one of said classification levels of information.

16. The system of claim 15 wherein that data card is an encryption means.

17. The system of claim 16 wherein the data cards includes an information security means.

18. The system of claim 17 wherein the data card is a daughter card.

19. The system of claim 15 wherein the means of reallocating at least one of the processors dynamically reallocates said processors.

20. The system of claim 15 wherein the classification levels are TOP SECRET, SECRET and CONFIDENTIAL.

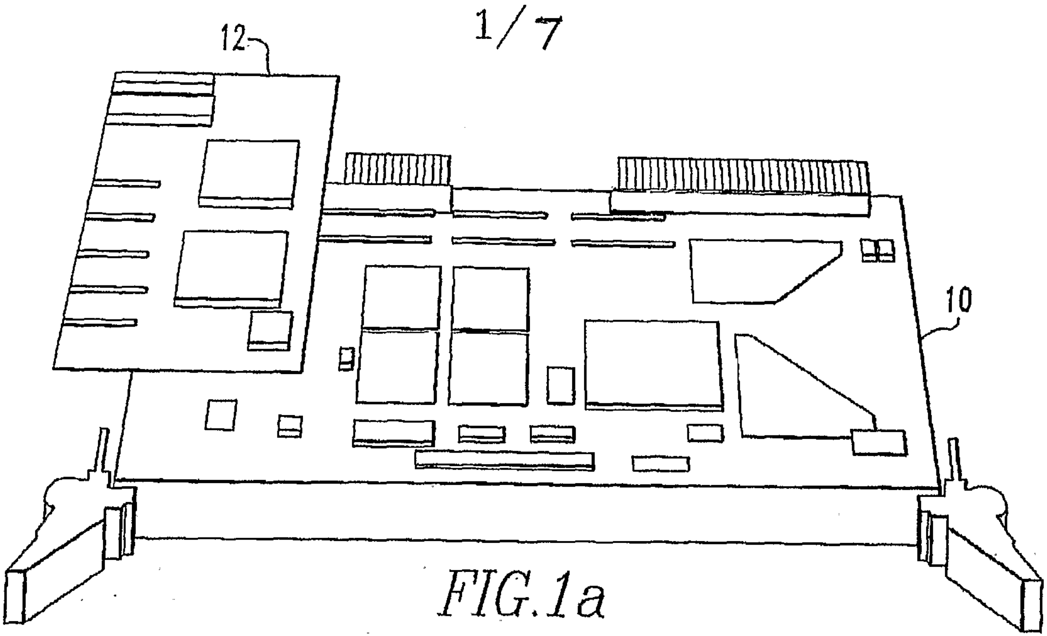

12
10

FIG.1a

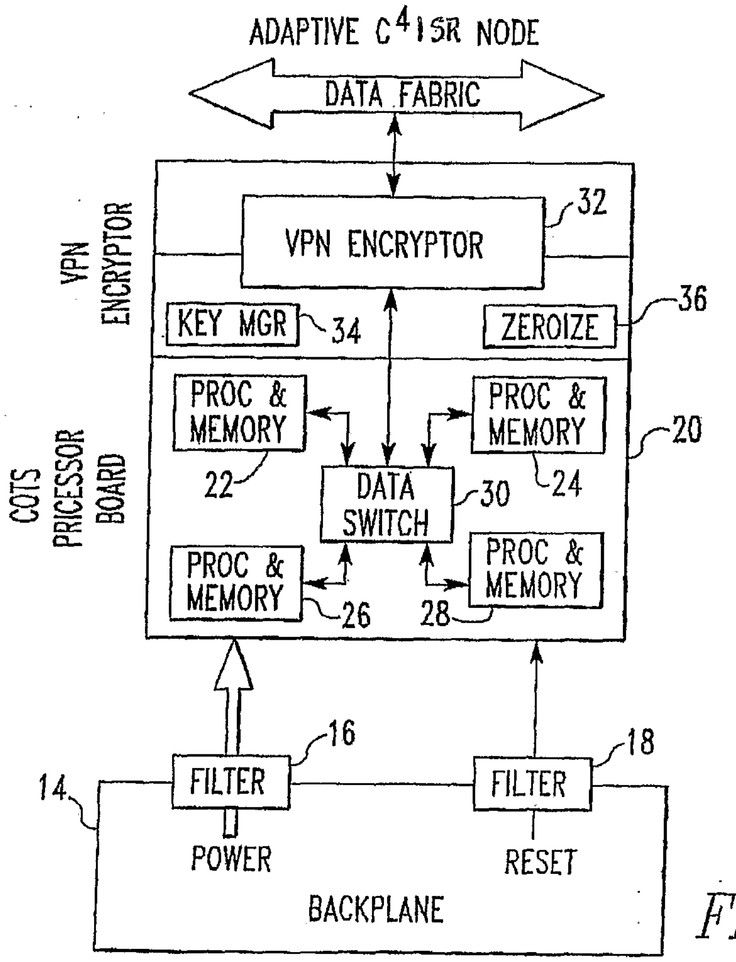

ADAPTIVE C4ISR NODE
DATA FABRIC
VPN ENCRYPTOR
VPN ENCRYPTOR
32
KEY MGR
34
ZEROIZE
36
COTS PROCESSOR BOARD
PROC & MEMORY
22
PROC & MEMORY
24
20
DATA SWITCH
30
PROC & MEMORY
26
PROC & MEMORY
28
16
FILTER
18
FILTER
14
POWER
RESET
BACKPLANE

FIG.1b

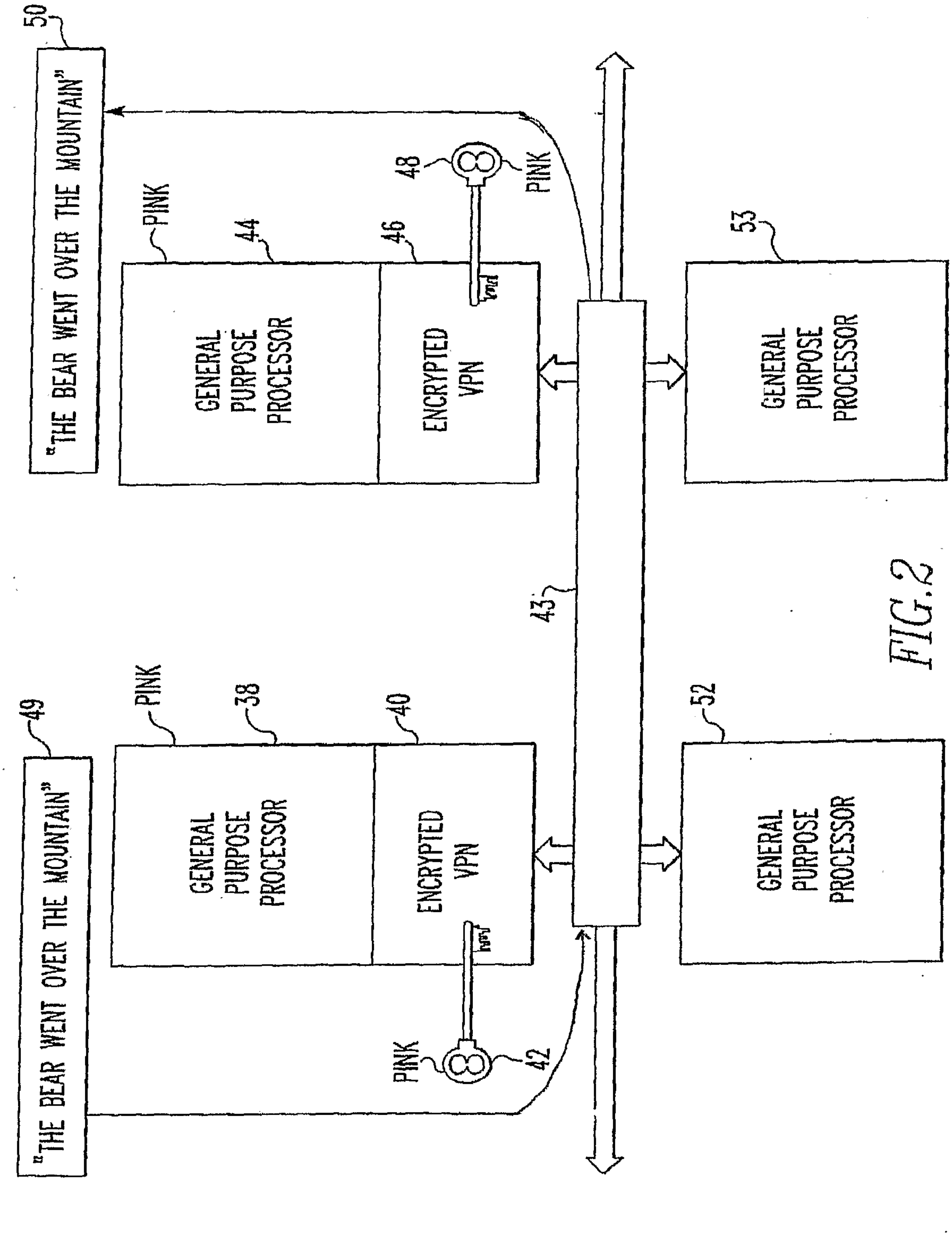

50
"THE BEAR WENT OVER THE MOUNTAIN"
PINK
44
GENERAL PURPOSE PROCESSOR
46
ENCRYPTED VPN
48
PINK
53
GENERAL PURPOSE PROCESSOR
43
49
"THE BEAR WENT OVER THE MOUNTAIN"
PINK
38
GENERAL PURPOSE PROCESSOR
40
ENCRYPTED VPN
PINK
42
52
GENERAL PURPOSE PROCESSOR

FIG.2

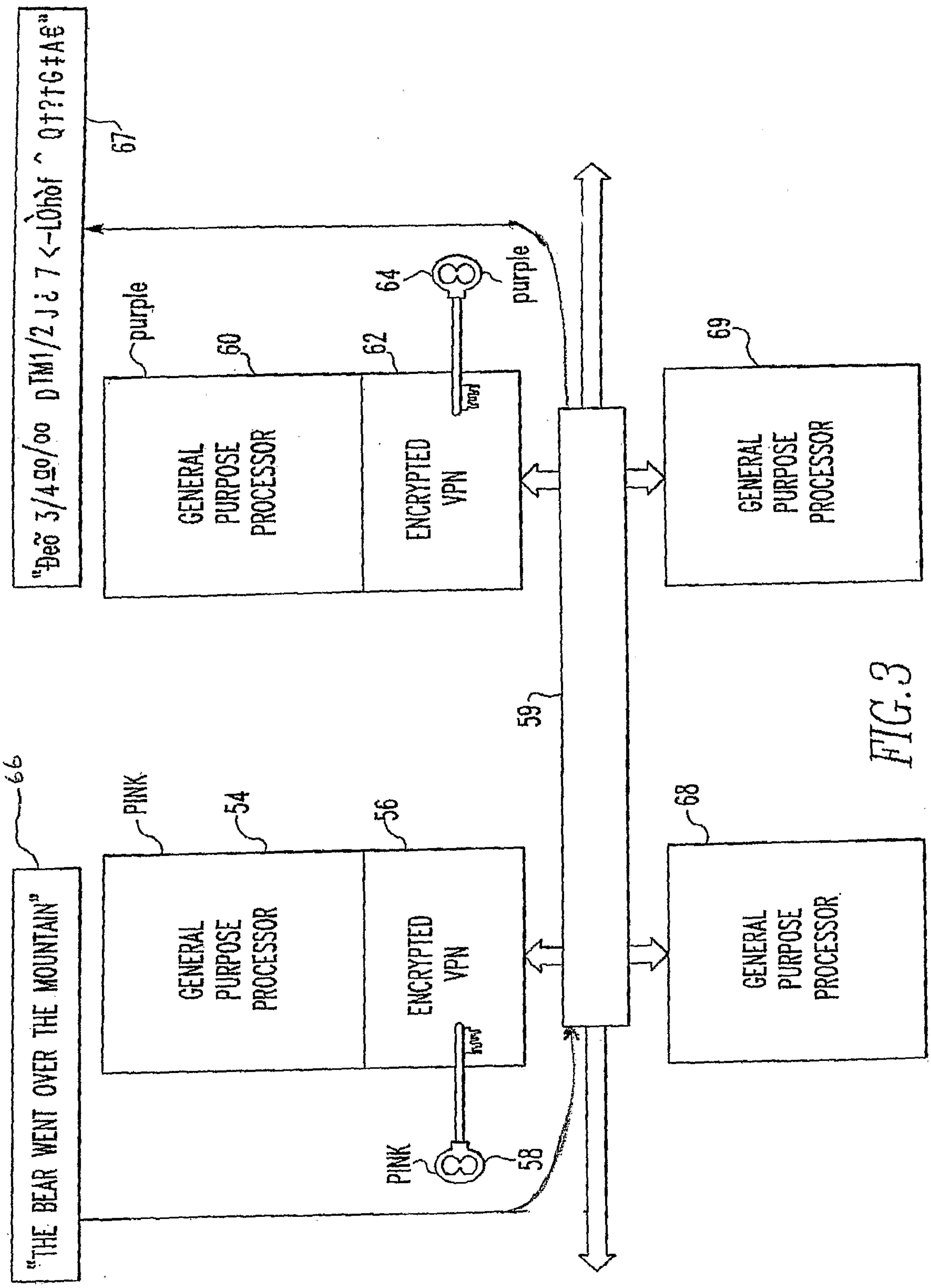

"THE BEAR WENT OVER THE MOUNTAIN"
66
PINK
54
56
GENERAL PURPOSE PROCESSOR
ENCRYPTED VPN
PINK
58
"Ðeõ 3/4º/oo DTM1/2 J ¿ 7 <-LÒhòf ^ Q†?†G‡Aɞ"
67
purple
60
62
GENERAL PURPOSE PROCESSOR
ENCRYPTED VPN
64
purple
purple
59
68
GENERAL PURPOSE PROCESSOR
69
GENERAL PURPOSE PROCESSOR

FIG.3

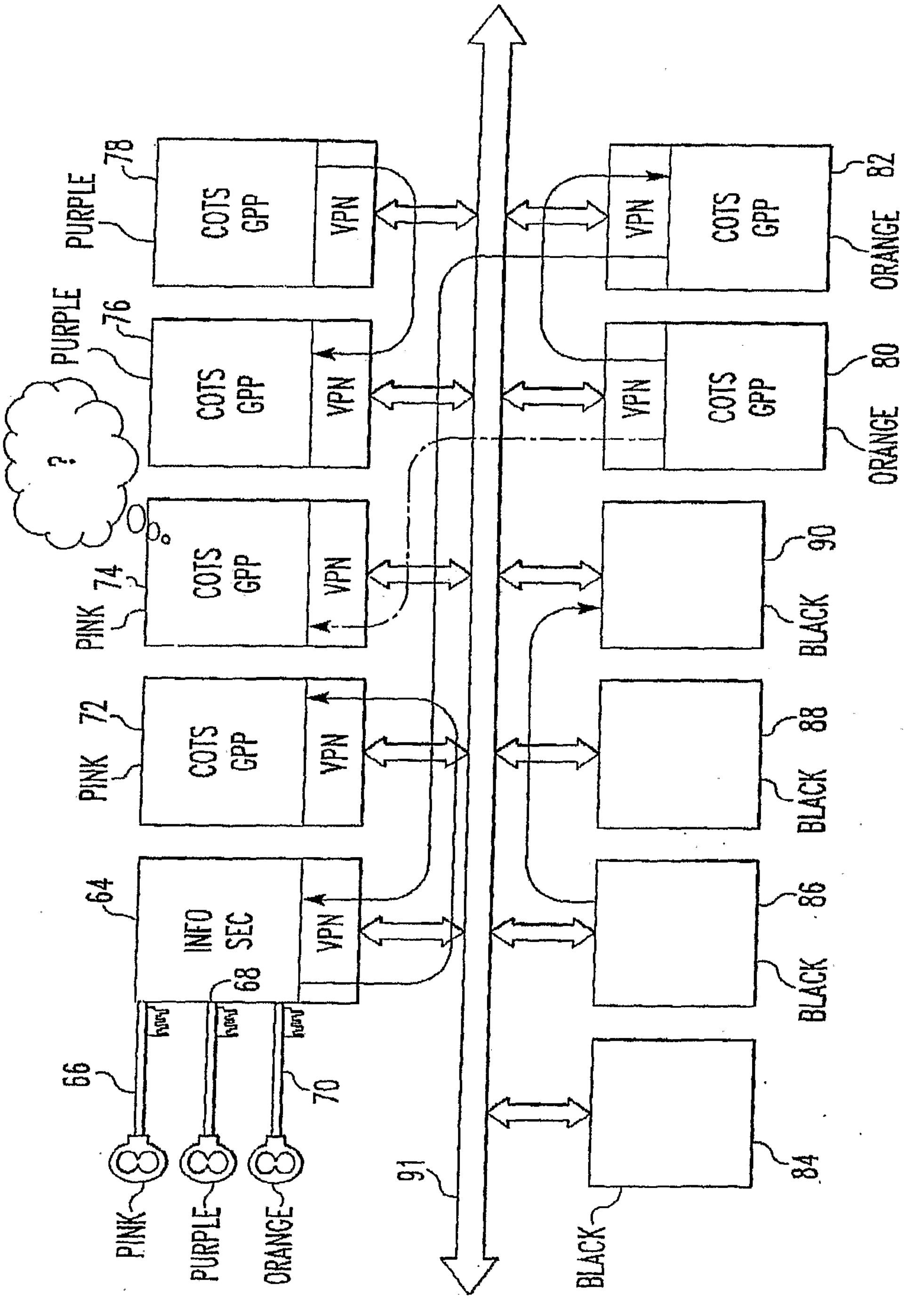

PINK
PURPLE
ORANGE
66
68
70
64
INFO SEC
VPN
PINK
72
COTS GPP
VPN
PINK
74
COTS GPP
VPN
?
PURPLE
76
COTS GPP
VPN
PURPLE
78
COTS GPP
VPN
91
BLACK
84
BLACK
86
BLACK
88
BLACK
90
ORANGE
80
COTS GPP
VPN
ORANGE
82
COTS GPP
VPN

FIG. 4

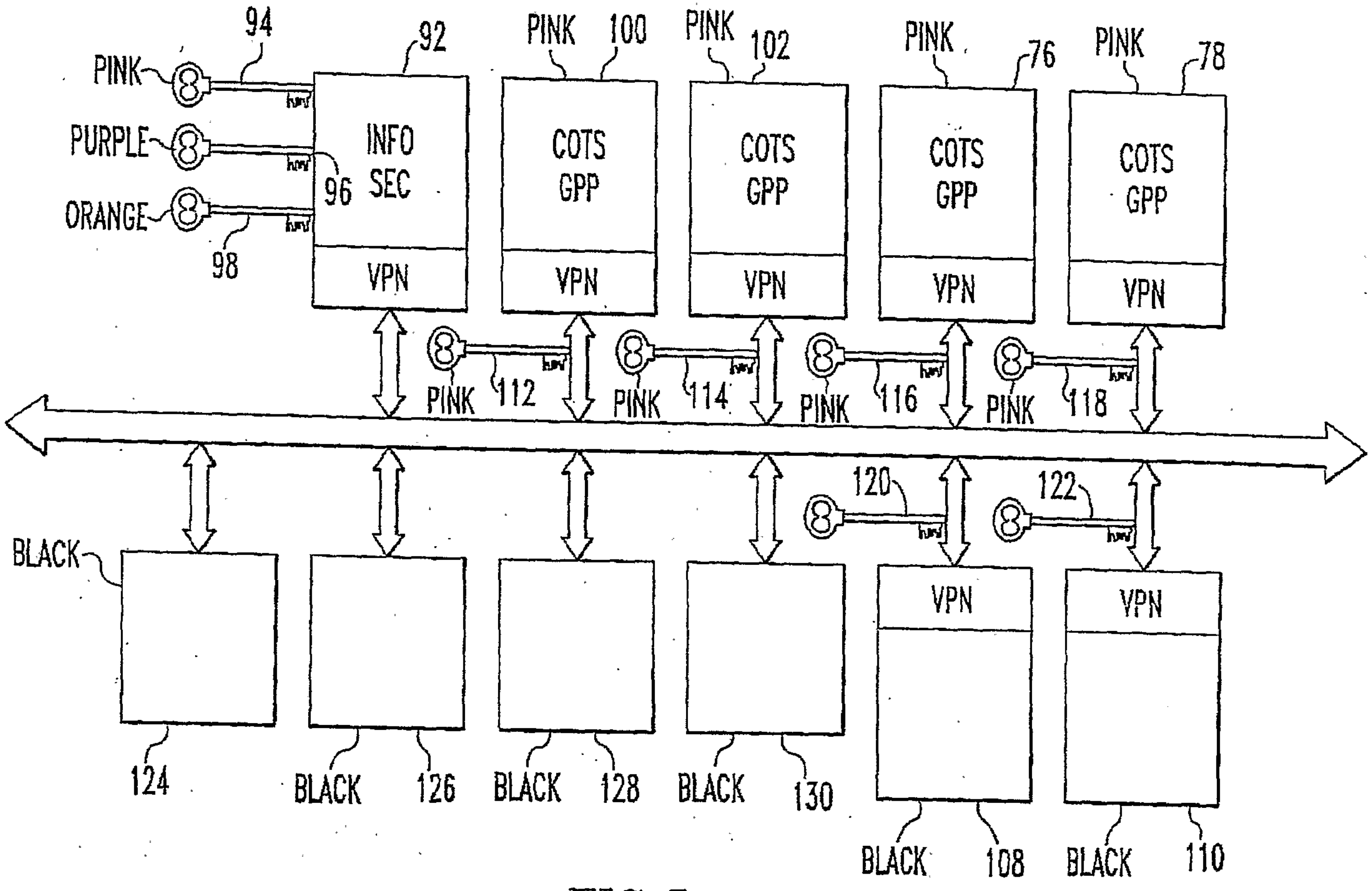

94
PINK
PURPLE
ORANGE
98
96
92
INFO
SEC
VPN
PINK
100
COTS
GPP
VPN
PINK
102
COTS
GPP
VPN
PINK
76
COTS
GPP
VPN
PINK
78
COTS
GPP
VPN
PINK
112
PINK
114
PINK
116
PINK
118
120
122
VPN
VPN
BLACK
124
BLACK
126
BLACK
128
BLACK
130
BLACK
108
BLACK
110

FIG.5

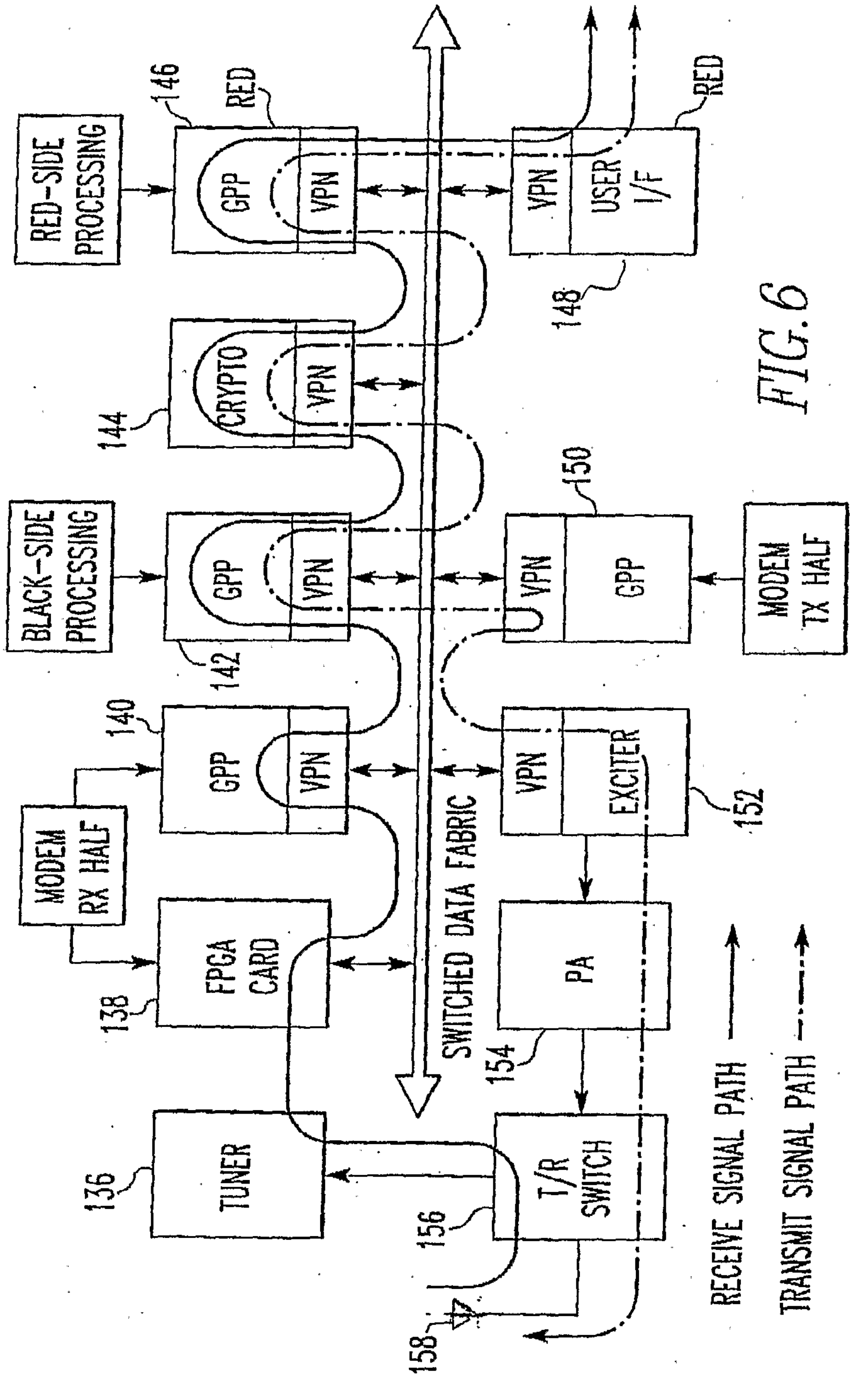

RED-SIDE PROCESSING
146
RED
GPP
VPN
VPN
USER I/F
RED
148
CRYPTO
VPN
144
BLACK-SIDE PROCESSING
GPP
VPN
142
150
VPN
GPP
MODEM TX HALF
MODEM RX HALF
GPP
VPN
140
VPN
EXCITER
152
FPGA CARD
138
SWITCHED DATA FABRIC
PA
154
TUNER
136
T/R SWITCH
156
158
RECEIVE SIGNAL PATH
TRANSMIT SIGNAL PATH

FIG.6

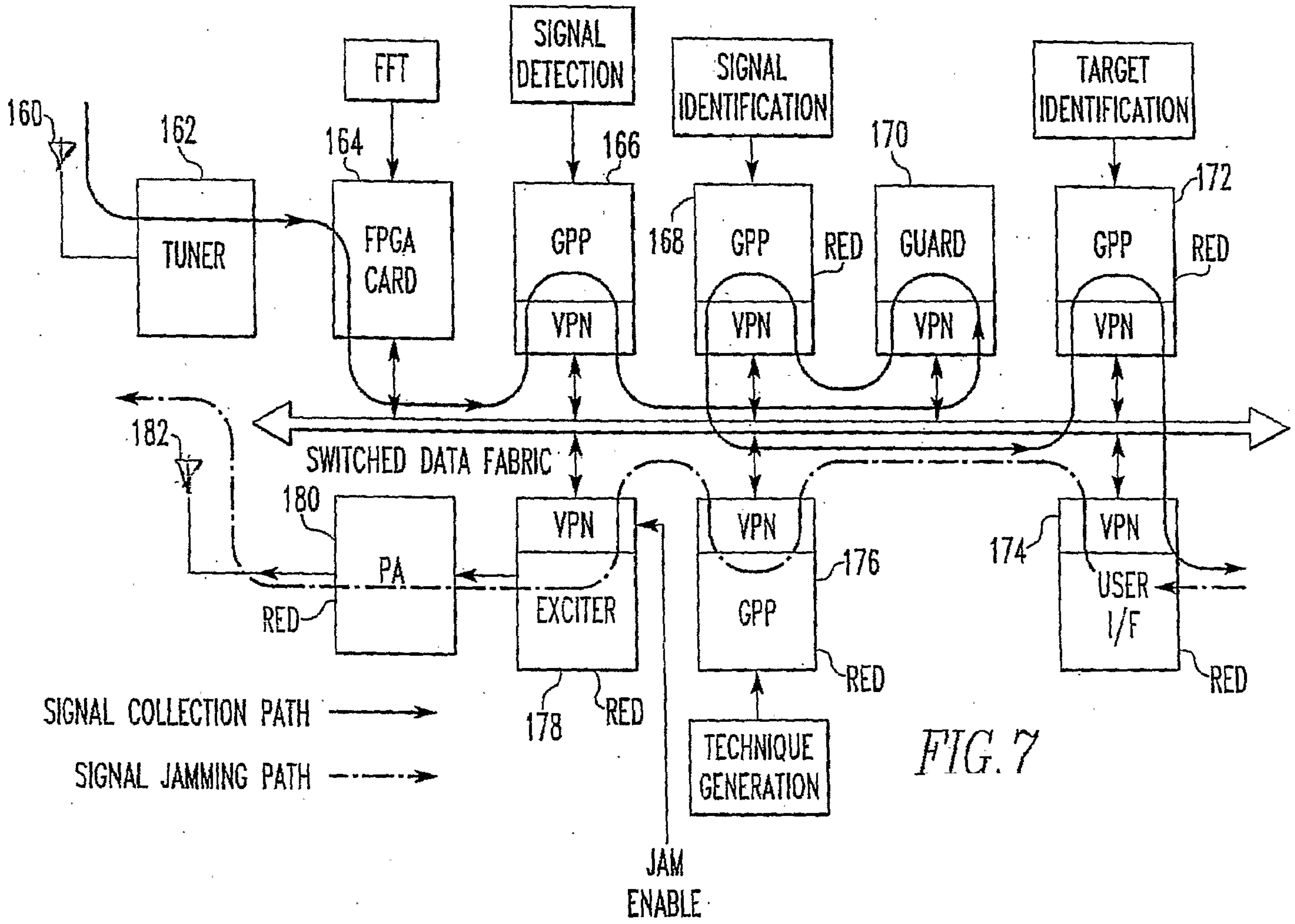

160
162
TUNER
164
FPGA CARD
FFT
SIGNAL DETECTION
166
GPP
VPN
SIGNAL IDENTIFICATION
168
GPP
VPN
RED
170
GUARD
VPN
TARGET IDENTIFICATION
172
GPP
VPN
RED
SWITCHED DATA FABRIC
182
180
PA
RED
VPN
EXCITER
178
RED
JAM ENABLE
VPN
GPP
176
RED
TECHNIQUE GENERATION
174
VPN
USER I/F
RED
SIGNAL COLLECTION PATH
SIGNAL JAMMING PATH

FIG. 7