

(12) PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. AU 199659966 B2
(10) Patent No. 712703

(54) Title
Process and device for transmitting confidential connection and service information between subscriber terminals and one or more digital exchanges

(51)⁶ International Patent Classification(s)
H04Q 011/04 H04L 029/06

(21) Application No: **199659966**

(22) Application Date: **1996.06.08**

(87) WIPO No: **WO96/42182**

(30) Priority Data

(31) Number	(32) Date	(33) Country
19521485	1995.06.13	DE

(43) Publication Date : **1997.01.09**

(43) Publication Journal Date : **1997.02.27**

(44) Accepted Journal Date : **1999.11.11**

(71) Applicant(s)
Deutsche Telekom AG

(72) Inventor(s)
Helmut Stolz

(74) Agent/Attorney
CULLEN and CO,GPO Box 1074,BRISBANE QLD 4001

(56) Related Art
"ENCRYPTION AND ISDN..." O'HIGGINS ETAL. IEEE 1987 PP863-869
"INTEGRATING CRYPTOGRAPHY IN ISDN (PRESSTUN) 16-20 AUG. 1987
ADVANCES IN CRYPTOLOGY - CRYPTO '87 VOL.7 PP9-18



(51) Internationale Patentklassifikation ⁶ : H04Q 11/04, H04L 29/06		A1	(11) Internationale Veröffentlichungsnummer: WO 96/42182
			(43) Internationales Veröffentlichungsdatum: 27. December 1996 (27.12.96)
(21) Internationales Aktenzeichen: PCT/DE96/01068		(81) Bestimmungsstaaten: AU, CA, IS, JP, NO, NZ, TR, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
(22) Internationales Anmeldedatum: 8. Juni 1996 (08.06.96)			
(30) Prioritätsdaten: 195 21 485.4 13. Juni 1995 (13.06.95) DE		Veröffentlicht <i>Mit internationalem Recherchenbericht.</i> <i>Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>	
(71) Anmelder (für alle Bestimmungsstaaten ausser US): DEUTSCHE TELEKOM AG [DE/DE]; Godesberger Allee 87-91, D-53105 Bonn (DE).			
(72) Erfinder; und			
(75) Erfinder/Anmelder (nur für US): STOLZ, Helmut [DE/DE]; Am Gensberge 12, D-57080 Sieben (DE).			
(74) Anwalt: KAMPFENKEL, Klaus; Sonnenberger Strasse 100, D-65193 Wiesbaden (DE).			

(54) Title: PROCESS AND DEVICE FOR TRANSMITTING CONFIDENTIAL CONNECTION AND SERVICE INFORMATION BETWEEN SUBSCRIBER TERMINALS AND ONE OR MORE DIGITAL EXCHANGES

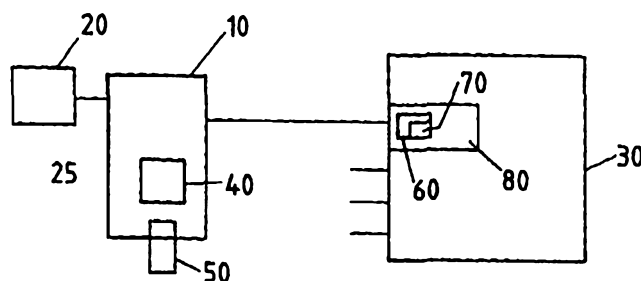
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ÜBERTRAGUNG VON VERTRAULICHEN VERBINDUNGS-AUFBAU- UND SERVICEINFORMATIONEN ZWISCHEN TEILNEHMERSEITIGEN ENDEINRICHTUNGEN UND EINER ODER MEHREREN DIGITALEN VERMITTLUNGSSTELLEN

(57) Abstract

The invention relates to a process and a device for transmitting confidential and authentic connection and/or service information between subscribers' data terminals and one or more exchanges of a digital communication system. As this confidential information is transmitted between a subscriber's terminal and an exchange in plain language, i.e. uncoded, there is the risk that intruders or eavesdroppers may receive this information. It is therefore the aim of the invention to make misuse of the exchange and prejudice to the subscriber by an unauthorised person difficult or even completely impossible. To this end the invention provides a process and a device in which there is at least one first security device at at least one subscriber, there is at least one second security device in the exchange or, alternatively, prior to each exchange there is an additional device in which there is at least one second security device. The first and second security devices can encode and/or decode the subscriber's connection and/or service information and exchange it between them.

(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren sowie eine Vorrichtung zur Übertragung von vertraulichen und authentischen Verbindungsaufbau- und/oder Serviceinformationen zwischen teilnehmerseitigen Datenendeinrichtungen und einer oder mehreren Vermittlungsstellen eines digitalen Kommunikationsnetzes. Da diese vertraulichen Informationen im Klartext, d.h. unverschlüsselt, zwischen einem Teilnehmeranschluß und einer Vermittlungsstelle übertragen werden, besteht die Gefahr, daß Eindringlinge bzw. Lauscher diese Informationen abhören können. Der Erfindung liegt daher die Aufgabe zugrunde, einen Mißbrauch der Vermittlungsstelle sowie eine Schädigung des Teilnehmeranschluß-Inhabers durch einen nichtberechtigten Eindringling zu erschweren oder sogar völlig zu beseitigen. Dazu stellt die Erfindung ein Verfahren und eine Vorrichtung zur Verfügung, die dadurch gekennzeichnet sind, daß wenigstens bei einem Teilnehmer wenigstens eine erste Sicherheitseinrichtung angeordnet ist, daß wenigstens in der Vermittlungsstelle wenigstens eine zweite Sicherheitseinrichtung angeordnet ist oder alternativ dazu jeder Vermittlungsstelle eine Zusatzeinrichtung vorgeschaltet ist, in der wenigstens eine zweite Sicherheitseinrichtung angeordnet ist, wobei die erste und die zweite Sicherheitseinrichtung Verbindungsaufbau- und/oder Serviceinformationen des Teilnehmers ver- und/oder entschlüsseln und untereinander austauschen können.



Process and device for transmitting confidential connection establishment and service information between subscriber terminals and one or more digital exchanges

5 The invention concerns a process for the transmission of confidential and authentic connection establishment and/or service information between subscriber-side terminals and one or more digital exchanges of a digital communication network, in particular an ISDN network,
10 according to claim 1, as well as a device for the transmission of confidential connection establishment and service information according to claim 6 and 8.

15 Digital telecommunication networks are known that feature a plurality of subscriber connections and digital exchanges. Since a subscriber connection transmits all dialing and service information unencoded, i.e., as plain text to a digital exchange intruders or eavesdroppers can simply tap into this confidential information on the
20 subscriber lines by cutting into existing communication paths on intruding into the existing lines at different points. An intruder, once having obtained said dialing and service information, can use the exchange at the expense of the subscriber, even without being authorized
25 to do so.

Therefore, the object of the invention is to make misuse of the exchange by unauthorized intruders at the expense of authorized subscriber connection owners difficult or
30 even impossible.

This object is achieved by the invention through the steps of process claim 1 and the features of device claims 6 and 8.

35

The invention is implemented in a digital communication network, in particular an ISDN. Such a digital communication network includes, as is known, a plurality



of exchanges, at least one network terminator installed at the subscriber, to which at least one data terminal, such as telephone sets, personal computers, or fax machines, can be connected. Undesired use of an exchange by an intruder is prevented by providing at least one first security device at a subscriber connection owner; in addition, at least one second security device is provided in at least one exchange, with the first and second security device assigned to a specific subscriber being capable of encoding and/or decoding and exchanging with each other connection establishment and/or service information. Each of said security devices has a security module capable of receiving an identification carrier.

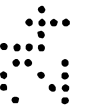
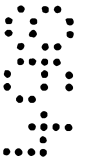
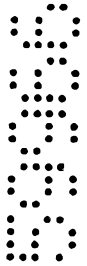
Connection-specific assemblies, each containing a second security device, are installed at each exchange. This embodiment is, however, expensive and complex, since the exchanges themselves must be rebuilt.

A more cost-effective method, which can be implemented in a simpler manner, consists of installing an additional device, based on the existing digital exchanges, between the network terminators assigned to the exchange and the exchange. The respective second security device for each subscriber connection is installed in this additional device.

The first security device of a given connection owner is advantageously arranged in the network terminator itself corresponding to each subscriber connection. In this case a single security device is sufficient even if the owner of a subscriber line can connect up to eight data terminals to the network termination via an S_0 bus. It is perfectly possible to equip each data terminal of a given network termination with its own security device. Another alternative may consist of connecting a security device between each data terminal and its network



terminator. It can be easily seen, however, that both of the latter implementation options are complex and costly, since each data terminal requires its own security device. The service information may include call forwarding and conferencing functions, for example. If the



digital communication network is an ISDN, the transmission of confidential information between the subscriber-side first security device and the respective second security device in the exchange takes place via the D channel of the ISDN network. Each
5 identification carrier can then store an individual cryptographic key that is specific to a given subscriber connection owner. The identification carrier may be a smart card that can be inserted by the owner of a subscriber connection in the first security device and by an employee of the network operator in the second
10 security device. An advantageous alternative provides a software module as the identification carrier, which can be installed exchangeably in the respective security device. In an advantageous refinement, the identification carrier is a software module, which can be exchangeably installed in the respective
15 security module. In an advantageous refinement, the first, subscriber-side, security device and the second security device of the exchange can perform subscriber authentication to the exchange. Alternatively, separate authentication devices can be installed for this function.
20 Protection for the exchange and the authorized subscriber connection owner can be enhanced by having the first and second security devices, assigned to a given subscriber, encode and decode, respectively, a user-to-user communication to be
25 transmitted via the control channel of the digital communication network.

The subscriber-side security device of a given subscriber and the security device of the exchange preferably have the same
30 subscriber-specific ID. In addition, they encode and decode the confidential information with the same subscriber-specific key.

The invention is explained below with reference to the embodiments illustrated in the drawing.



Fig. 1 schematically shows a section of a digital communication network shown as a communication path from a telephone set to a digital exchange where the invention is implemented,

5

Fig. 2 shows one embodiment where the security device according to this invention is installed in an additional device on the exchange side,

10 Fig. 3 shows a detailed block diagram of the network terminator with the security device according to this invention, and

15 Fig. 4 shows a detailed block diagram of a connection-specific assembly in the exchange with a built-in security module,

Fig. 5 shows the frame format of the ISDN bit streams,

20 Fig. 1 shows in a simplified form a part of a digital communication network, exemplified in the description that follows as an ISDN network. A telephone set 20 is illustrated as a data terminal on the subscriber side, which is connected to a network terminator 10 via an S_0 bus 25. Network terminator 10, 25 also referred to as Net Terminator (NT), can be installed in the building or room of a subscriber connection owner. Up to eight data terminals, such as other telephone sets 20, fax machines, or personal computers, can be connected to S_0 bus 25. In the example illustrated, a subscriber-side security device 40, 50 according 30 to this invention is built into network terminator 10. The safety device includes a subscriber-specific identification carrier 50 and a safety module 40, which can be permanently installed in



network terminator 10 where an identification carrier 50 can be inserted. Identification carrier 50 can be a smart card or a software module. Security device 40 and identification carrier 50 are designed so that they can encode or decode confidential connection establishment or service information with a subscriber-specific or connection-specific key. This key can be stored in a storage module of the smart card of the connection owner. The output of network terminator 10 is connected to a corresponding ISDN exchange 30 via a twisted two-wire cable in a known manner. Of course, an ISDN network includes a plurality of network terminators 10 and a plurality of exchange systems 30, which may be interconnected via twisted two-wire cables. In the future, conventional two-wire cables can be supplemented and replaced by fiber-optic cables, for example. Exchange 30 includes a plurality of assemblies 80 (Fig. 1 only illustrates a single connection-specific assembly 80), each assigned to certain subscriber connection owners. In the first embodiment according to this invention, a security device 60, 70 is arranged in each connection-specific assembly 80. Like the subscriber-specific security device 40, 50, security device 60, 70 in exchange 30 includes a module 60, which can be permanently installed in assembly 80 and an identification carrier 70, which can be inserted therein. It is assumed that identification carrier 70 in exchange 30 also contains the ^{individual} cryptographic key of subscriber-side security device 40, 50.

Fig. 2 shows an alternative embodiment where additional device 100 is connected between network terminator 10 and exchange 30. For greater clarity, Fig. 2 shows additional device 100 only with the built-in security device 60, 70. Normally all security devices 60, 70 of subscribers or network terminators jointly served by exchange 30 are installed in additional device 100. The



corresponding subscriber lines are indicated in Figs. 1 and 2. Again, identification carriers 70 can be inserted as smart cards from the outside by an operator or, in the implementation as a software module, can be installed in the respective security module 60. The use of additional device 100 has the advantage that existing ISDN network exchanges can continue to be used without time-consuming, costly, and complex modifications of the exchange system for the encoded transmission of confidential information, for example, of the subscriber of telephone set 20 to exchange 30.

Fig. 3 shows a simplified block diagram of the known network terminator 10, where the security module 40 according to this invention, together with identification carrier 50, are installed. On the subscriber side, network terminator 10 has a connection unit for S_0 bus 25, to which up to eight data terminals 20 can be connected. Since the structure and the mode of operation of network terminator 10 are generally known, only the essential components are briefly explained below. Basically network terminator 10 has a send path and a receive path. The send path includes an encoder 210, which, among other things, supplies the confidential information to be transmitted in the D channel of the ISDN network to an encoder in security device 40, 50, and a multiplexer 200, which combines the two B channels and the D channel to a continuous data stream in a time multiplexing operation. A suitable frame format consists of 48 bits per 250 ms, with only four D channel bits provided per frame. In other words, 16 kbits/sec are transmitted over the D channel (see Fig. 5). The send path then goes to a hook switch 170 via a transmitter 180; said hook switch sends the outgoing data stream to a two-wire cable that connects exchange 30 to network terminator 10. Incoming data streams go through hook switch 170, a receiver 160, and a device 150, which equalizes and amplifies



the data stream received and recovers the clock signal from it. Then the data stream passes through a demultiplexer 140, which decomposes the data stream again into the two B channels and the D channel. The demultiplexed data stream passes through decoder 130 and is then transmitted, according to a destination address, to telephone set 20, for example, via the S_0 bus 25. An echo compensation 190, connected in parallel between transmitter 180 and receiver 160, is used, among other things, for compensating outgoing messages sent to the receive path through hook switch 170 and receiver 160. The heart of network terminator 10 is a controller 220, which controls the management and mutual control of the individual components. The security module 40 according to this invention with the inserted identification carrier 50 is connected, for example, to controller 220, encoder 210, multiplexer 200, demultiplexer 140, and decoder 130. Controller 220 is also responsible for activating or deactivating security device 40, 50 as required by the situation.

Fig. 4 shows an example of a block diagram of a subscriber-specific assembly 80, installed in exchange 30. The connection-specific assembly 80 basically forms the counterpart of network terminator 10. Incoming data messages go, via the two-wire line, to a hook switch 230 and then pass through a demultiplexer 240, a decoder 250, and a D channel handler 260. D channel handler 260 supplies control information to a central controller of exchange 30. In the opposite direction, outgoing messages pass through an encoder 270, a multiplexer 290, and a hook switch 230 on the two-wire line to network terminator 10. Also in connection-specific assembly 80, a controller 280 is responsible for the management of and interaction between the individual components. Security module 60 is installed in connection-specific assembly 80, according to this invention, with a smart card that can be



inserted from the outside, or an installed software module 70. Security device 60, 70 which includes security module 60 and identification carrier 70, is connected to encoder 270, decoder 250, D channel handler 260, and controller 280. As mentioned previously, authentication device 60, 70 can also be advantageous by installed in additional device 100, as shown in Fig. 2.

It is convenient to install security device 40, 50 in network terminator 10 itself, since in this way only one security device 40, 50 is required, regardless of the number of data terminals 20 connected. However, it is also conceivable to arrange the subscriber-side security device 40, 50 in each data terminal 20. Another alternative consists of providing a security device (not illustrated) between network terminator 10 and each connected data terminal 20. For reasons of economics, it is convenient to install security devices 40, 50 in network terminator 10 itself, shown in Fig. 1. Then identification carrier 50 can be installed in the form of a software module by the network operator when network terminator 10 is installed at the subscriber. If identification carrier 50 is a smart card, the subscriber can purchase this card, containing the subscriber's individual subscriber key, from the network operator.

The transmission of confidential connection establishment and/or service information between telephone set 20 and exchange 30 is now described in detail.

It is assumed that one subscriber-side security device 40, 50 is installed in network terminator 10 and a second security device 60, 70 is installed in assembly 80, assigned to the subscriber of telephone set 20 in exchange 30. According to the embodiment



illustrated in Fig. 2, security device 60, 70 can also be installed in additional device 100. The procedures described below occur basically in the same way in both cases.

Let us also assume that the subscriber-side identification carrier 50 and the exchange-side identification carrier 70 have the same ID, i.e., the identity of the subscriber of telephone set 20. In addition, subscriber-side security device 40, 50 and exchange-side security device 60, 70 have the same cryptographic key associated with the subscriber of telephone set 20. Both identification carriers 50, 70 are smart cards.

After security device 40, 50 has authenticated the subscriber of telephone set 20 to exchange 30 connected to security device 60, 70 installed in subscriber-specific assembly 80 - the authentication can be performed by separate authentication devices - all connection establishment and service information is encoded by the subscriber-side security device 40, 50 with the subscriber-specific key and transmitted to security device 60, 70 in the subscriber-specific assembly in the D channel via the ISDN network. Security device 60, 70 in exchange 30 decodes the received encoded connection establishment and/or service information with the common subscriber-specific key and sends the decoded information via the D channel handler to a central unit in exchange 30. In response to the decoded connection establishment information, the desired connection to the subscriber dialed is established and, in response to the decoded service information the requested services are made available. This ensures that an unauthorized intruder will not be able to establish a connection at the expense of the owner of the connection of telephone set 20. Different known encoding procedures can be used for encoding and decoding, such as, for example, the Rivest-Shamir-Adleman method or the Data Encryption



Standard method.

Let us now assume that instead of the smart card, a special encoding and decoding module 70 is installed in subscriber-specific assembly 80. Prior to encoding the confidential connection establishment and service information and transmitting it via the ISDN network to exchange 30, decoding module 70 is provided with the key assigned to the subscriber of telephone set 20 by a central or decentralized encryption center. The key can be transmitted to security device 60, 70 via a data medium, such as a diskette, or by electronic data transmission. Important and known security aspects must be taken into account, especially in confidential and authenticated information transmission, so the subscriber-specific key does not become known to unauthorized third parties. After security device 60, 70 of assembly 80 has received the subscriber-specific cryptographic key, the confidential connection establishment and service information is transmitted as described above.

An advantageous refinement of the invention provides that the control channel (D channel) of the digital communication network serves as a data transmission line for user-to-user transmission, specifically between data terminal 20 and exchange 30.

In this case the subscriber-side security device 40, 50 is capable of encoding, for example, data transmitted by a personal computer and transmitting it to security device 60, 70 of exchange 30. Security device 60, 70, which can be installed in subscriber-specific assembly 80 or in additional device 100, can decode this data information and transmit it in conjunction with exchange 30, for example, via the Datex P network to the subscriber dialed.



THE CLAIMS DEFINING THE INVENTION ARE AS FOLLOWS:

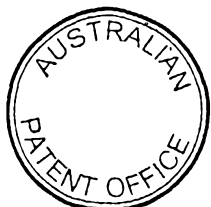
1. Process for the transmission of confidential connection establishment and/or service information
5 between subscriber-side data terminals (20) and one or more exchanges (30) of a digital communication network, with at least one subscriber-side network terminator (10), to which at least one data terminal (20) can be connected, with at least one security device (40, 50)
10 arranged at a subscriber, and at least one second security device (60, 70) assigned to the exchange (30), with the following process steps:
encoding and/or decoding the connection establishment and/or service information by the subscriber-side first
15 security device (40, 50);
transmission of the encoded connection establishment and/or service information between the first (40, 50) and second (60, 70) security device over a special control channel of the digital communication network;
20 encoding and/or decoding of the connection establishment and/or service information by the second security device (60, 70).
2. Process according to claim 1, characterized in
25 that the connection establishment and/or service information, establishes a connection to a dialed subscriber and/or makes the requested services available.
3. Process for transmission of confidential
30 connection



establishment and/or service information according to Claim 1 or 2,

characterized in that the connection establishment and/or service information is encoded and/or decoded with the same subscriber-specific key by the first (40, 50) and second (60, 70) security device.

- 
4. Process for transmission of confidential connection establishment and/or service information according to one of Claims 1 through 3, characterized in that authentication between the subscriber of the network terminator (10) and the respective exchange (30) is performed by the first security device (40, 50) and a second security device (60, 70) or by separate authentication devices prior to transmission of confidential connection establishment and/or service information.
- 
5. Process for transmission of confidential connection establishment and/or service information according to one of Claims 1 through 4, characterized in that the connection establishment and/or service information is transmitted via the D channel of an ISDN network.
6. Device for transmission of confidential connection establishment and/or service information between subscriber-side data terminals (20) and one or more exchanges (30) of a digital communication network with at least one subscriber-side network terminator (10), to which at least one data terminal (20) can be connected, characterized in that at least one first security device (40, 50) is arranged at at least one subscriber, and



at least one second security device (60, 70) is arranged at least in the exchange (30), with the first (40, 50) and second (60, 70) security devices being capable of encoding and/or decoding and exchanging with each other connection establishment and/or service information of the subscriber over a special control channel in the digital network.

7. Device for transmission of confidential connection establishment and/or service information according to claim 6, characterized in that the exchange (30) has a plurality of assemblies (80) assigned to certain subscribers, where a second security device (60, 70) is arranged.

8. Device for transmission of confidential connection establishment and/or service information between subscriber-side data terminals (20) and one or more exchanges (30) of a digital communication network with at least one subscriber-side network terminator (10), to which at least one data terminal (20) can be connected, characterized in that a first security device (40, 50) is arranged at at least one subscriber; an additional device (100) with a second security device (60, 70) is connected upstream from the (or each) exchange (30), with the first (40, 50) and second (60, 70) security devices being able to encode and/or decode and exchange with each other connection establishment and/or service information of the subscriber over a special control channel of the digital communication network.

9. Device for transmission of confidential connection establishment and/or service information according to one of claims 6 through 8, characterized in that

each security device has a least one security module (40, 60), which can receive an identification carrier (50, 70).

10. Device for transmission of confidential



connection establishment and/or service information according to one of claims 6 through 9,

characterized in that

the first security device (40, 50) is arranged in
5 the network terminator (10).

11. Device for transmission of confidential connection establishment and/or service information according to one of claims 6 through 9,

10 characterized in that

a first security device (40, 50) is arranged in each data terminal (20) connected to the network terminator (10).

12. Device for transmission of confidential connection establishment and/or service information according to one of claims 6 through 9,

characterized in that

a first security device (40, 50) is arranged between each data terminal and the respective network terminator (10).

13. Device for transmission of confidential connection establishment and/or service information according to one of claims 6 through 12,

characterized in that

the digital communication network is an ISDN network and the encoded information is transmitted between the first security device (40, 50) and the second security device (60, 70) via the control channel (D channel) of the ISDN network.

14. Device for transmission of confidential connection establishment and/or service information according to one of claims 9 through 13,

characterized in that

the identification carrier (50, 70) is a smart card or a software module capable of encoding and/or decoding the confidential information.



15. Device for transmission of confidential connection establishment and/or service information according to one of claims 6 through 14, characterized in that

5 the first (40, 50) and second (60, 70) security device assigned to a given subscriber have the same subscriber-specific ID and can encode and/or decode confidential information with the same subscriber-specific key.

10

16. Device for transmission of confidential connection establishment and/or service information according to one of claims 6 through 15, characterized in that

15 the first (40, 50) and second (60, 70) security device assigned to a given subscriber can encode and/or decode all the data to be transmitted over the control channel of the digital communication network.

20

DATED this 24th day of April 1998

DEUTSCHE TELEKOM AG

By their Patent Attorneys

CULLEN & CO.



59966/96

1/2

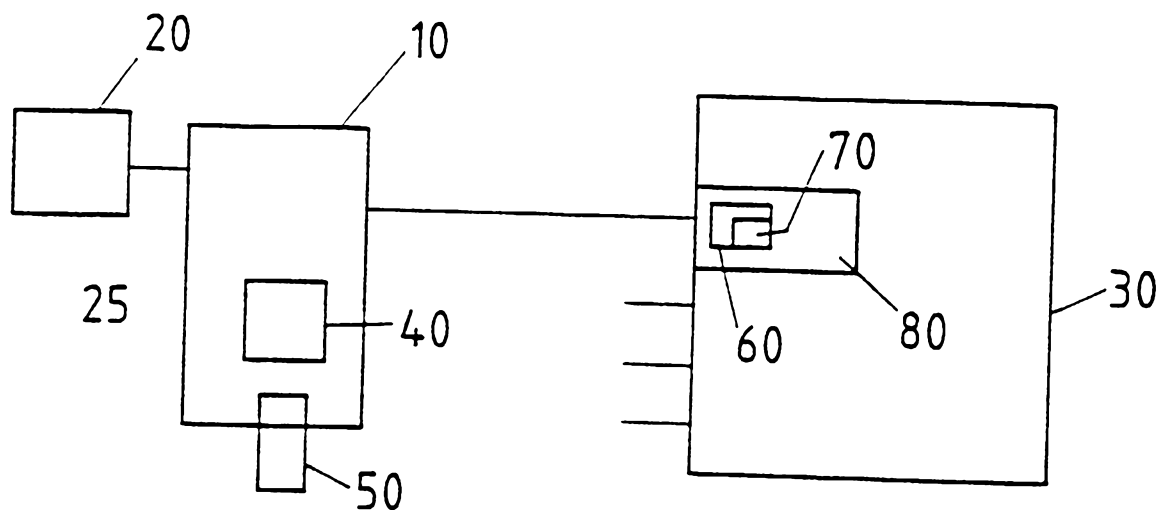


Fig. 1

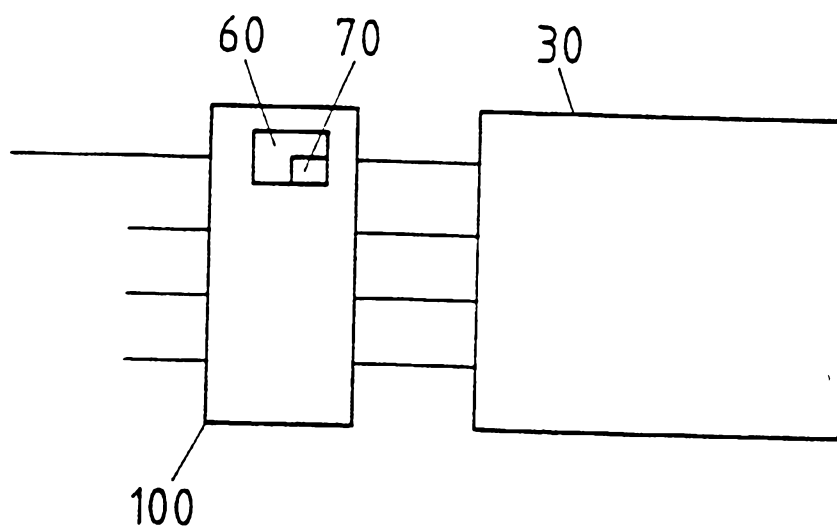


Fig. 2

1	1	8	1	1	1	1	1	8	1	1	1	8	1	1	1	8	1	1
F	L	B ₁	E	D	A	F	F	B ₂	E	D	S	B ₁	E	D	S	B ₂	E	D

Fig. 5

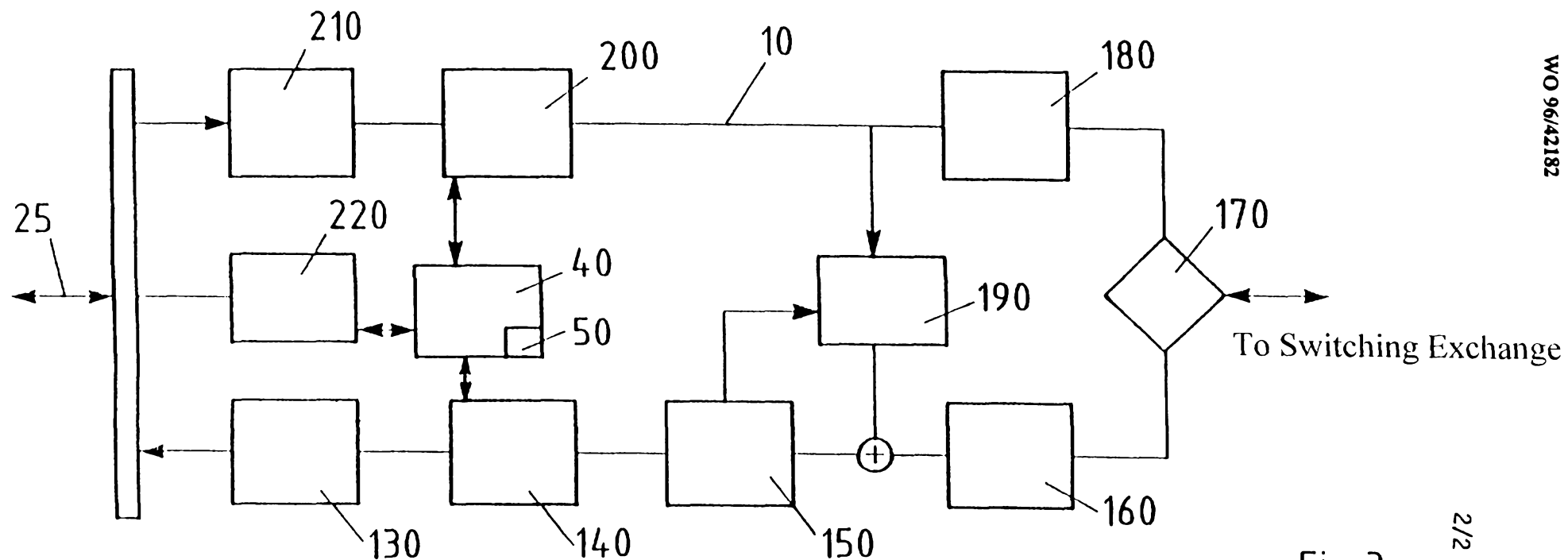


Fig. 3

2/2

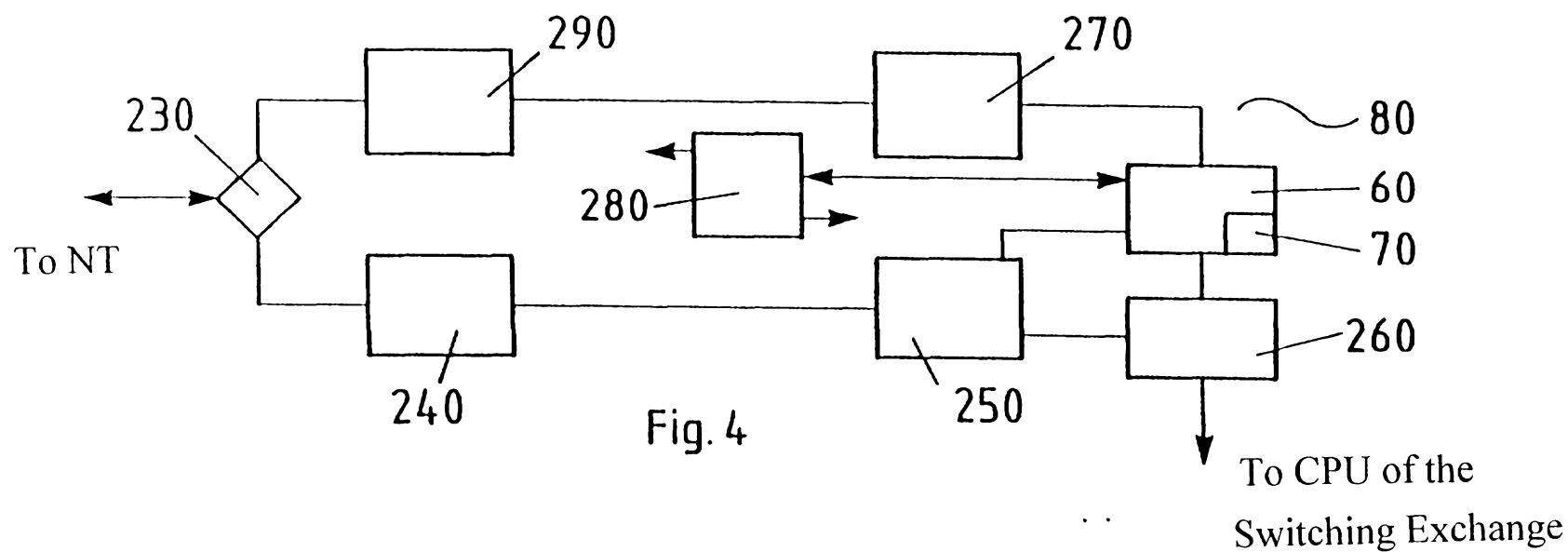


Fig. 4