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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 April 2001 (05.04.2001)

PCT

(10) International Publication Number
WO 01/23227 A1

(51) International Patent Classification[7]: B60R 25/00

(21) International Application Number: PCT/AU00/01186

(22) International Filing Date:
28 September 2000 (28.09.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 3123 28 September 1999 (28.09.1999) AU

(71) Applicant *(for all designated States except US)*: **AUSTRALIAN ARROW PTY LTD** [AU/AU]; 65 Lathams Road, Carrum Downs, Victoria 3201 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **JANKOWSKI, David, Paul** [AU/AU]; 5/4 Dennis Street, Clayton, Victoria 3168 (AU). **KERRY, Leonard, John** [AU/AU]; 3 Fulmar Street, Carrum Downs, Victoria 3201 (AU). **JAMES, Campbell, Richard** [AU/AU]; 11 Kunyung Road, Mt Eliza, Victoria 3930 (AU).

(74) Agent: **FREEHILLS CARTER SMITH BEADLE**; 101 Collins Street, Melbourne, Victoria 3000 (AU).

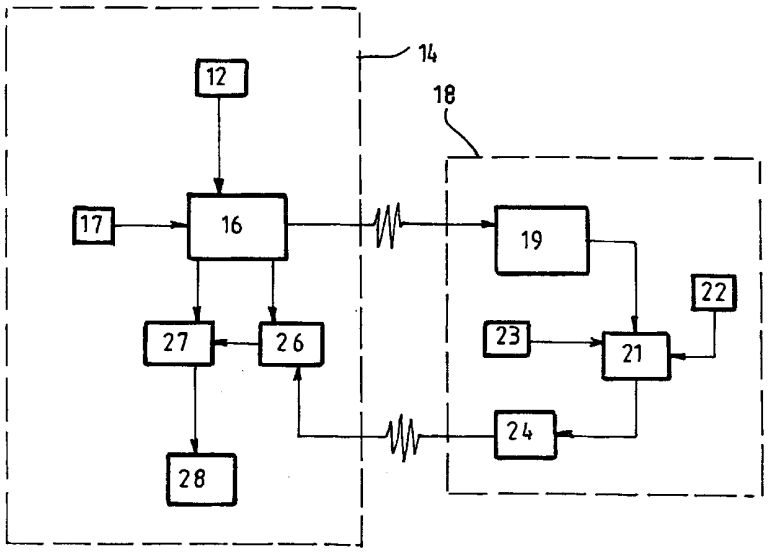
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE,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

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

Published:
— *With international search report.*

[Continued on next page]

(54) Title: IMPROVED SECURITY SYSTEM



(57) Abstract: A security system suitable for a vehicle (14) has a transponder (16) and a remote, portable device (18). The transponder (16) is associated with a random number generator (17) and incorporates a signal receiver (26) and a comparator (27). On actuation, the transponder generates a trigger signal which includes vehicle identification information and a random number. The portable device (18) receives and decodes the trigger signal and responds with a response signal which comprises one or more RF signals of a frequency and duration calculated by the device using a stored algorithm and a unique number in conjunction with the transmitted random number in the trigger signal. The frequency of the response signal is therefore varied until each different random number, and the receiver in the transponder is tuned to the expected response signal frequency.

WO 01/23227 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPROVED SECURITY SYSTEM

Field of the Invention

This invention relates to an improved security system and relates particularly to a security system which permits authorised keyless actuation of a locking system, a control system, or the like, to permit entry through or past a closure, such as a door, into a building, secure area or motor vehicle, or actuation of control circuits permitting operation of a motor vehicle or the like.

Background of the Invention

The invention will be described with particular reference to its application to a motor vehicle, but it will be understood that the principles of the invention apply to a wide range of applications.

Many forms of security systems have been proposed for motor vehicles which enable an authorised person to obtain access to the vehicle without the use of a key to physically unlock the vehicle doors. Such known systems include the provision of radio transmitter devices which, on actuation by a push button, cause the vehicle to unlock. These systems require the relatively bulky radio transmitter to be carried by the authorised person. Other systems, commonly known as "passive access" systems, enable an electronic identification device carried by an authorised person to actuate the locking mechanism of a locked vehicle. With such a system, the vehicle transmits a message to the electronic identification device when the person touches the vehicle door handle or triggers a short range proximity sensor in the vehicle. Typically, the message contains vehicle identification information so that the electronic identification device can determine whether or not to respond. The vehicle transmission may also contain a random number. If the vehicle identification code is correct, the random number is manipulated by the electronic identification device according to an algorithm. The result of the

manipulation is then transmitted to the vehicle which compares the response to an expected response. If the transmitted response and expected response match, the vehicle is unlocked.

The system may also include vehicle operation authentication whereby a similar process is repeated when the vehicle operator attempts to start the vehicle.

In this instance, it is desirable for the system to be able to determine whether or not the identification device is inside the vehicle. Therefore, typically, the vehicle's signal transmission is controlled so that it is unlikely that the identification device could detect the signal from outside the vehicle.

The known passive access system described above provides a remote keyless entry system which allows authorised entry to and operation of a vehicle by an authorised person, carrying the electronic identification device, simply walking up to the vehicle, opening the door and driving off. However, the system is vulnerable to an unauthorised person obtaining access to the vehicle. An attack on the security takes advantage of the contactless operation of the electronic identification device and the ability to activate that device remotely without the knowledge of the authorised owner. The attack works as follows:

The authorised owner of the vehicle locks the vehicle and walks away, beyond the normal range of communication between the electronic identification device and the vehicle communication system. A person carrying a transceiver follows the operator. Another person carrying a second transceiver stays with the vehicle. The person near the vehicle triggers the vehicle to transmit its identification message, such as by touching the door handle or triggering a proximity sensor in the vehicle. The transceiver carried by that person relays the vehicle's transmission to the transceiver of

the second person near the authorised operator. The electronic identification device carried by the authorised operator receives the relayed vehicle transmission and responds. This response is received by the transceiver carried by the person near the owner and the response is relayed back to the transceiver carried by the person near the vehicle which transmits the identification device response and the vehicle, receiving a valid response, unlocks the vehicle.

While proposals have been made to resolve the potential security problem, such proposals are relatively expensive and difficult to implement. One such proposal requires a further parameter to be determined, such as the distance between the vehicle and the electronic identification device, and the system is arranged so that the vehicle will only unlock if that distance is no greater than a predetermined maximum. While this additional proximity criteria is effective in most circumstances, it is a technically difficult and relatively expensive solution.

It is therefore desirable to provide an improved passive access security system which obviates the difficulties of the known system.

It is also desirable to provide an improved passive access security system which is relatively simple and economic to implement.

It is also desirable to provide an improved passive access security system which is robust and immune to attack using easily available, portable equipment such as transceivers.

Summary of the Invention

In accordance with one aspect of the invention there is provided a security system having transponder means adapted to be actuated to generate and transmit an electromagnetic trigger signal, and a portable electronic device

adapted to receive and respond to said trigger signal by transmitting a response signal, the receipt and authentication of which by the transponder means gives rise to a predetermined event, said response signal comprising one or more radio frequency signals of a frequency and duration determined by an algorithm together with a unique stored number with reference to a random number contained in the trigger signal.

In one embodiment of the security system of the invention incorporated into a motor vehicle, the transponder means is adapted to be actuated either by a proximity sensor or by a person touching the vehicle, lifting a door handle or otherwise signalling the transponder means. When an authenticated response signal is received by the transponder means, it causes the vehicle door or doors to become unlocked, in a known manner.

The present invention seeks to avoid unauthorised defeat by varying the communications between the transponder means and the portable electronic device. With present passive access systems as described above, the communication transmissions are of fixed frequencies and in relatively narrow bandwidths. With the present invention, the communication signals can be throughout a relatively broad spectrum of frequencies, such as from 200 MHz to 400 MHz, or even broader. With such a possible bandwidth, it is virtually impossible for a person with a transceiver or similar device to monitor, detect and retransmit the response signal. A person attempting to defeat the system would need to relay the entire 200 MHz band to an accomplice, but the wide bandwidth coupled with the low level of the target signal make implementation extremely unlikely.

In one form of the invention, the use of an algorithm with a unique stored number to manipulate the random number contained in the trigger signal means that both the frequency of the response signal and the number and length of

transmitted pulse trains can be varied. The transponder means is able to tune its receiver to the frequencies of the expected response signal.

In order that the invention is more readily understood, one embodiment will now be described with reference to the accompanying drawings.

Description of the drawings

Figure 1 is a schematic view of a vehicle incorporating a security system in accordance with the invention, and

Figure 2 is a block diagram schematically illustrating the features of the invention.

Description of the Preferred Embodiment

Referring to the drawings, in the embodiment illustrated, a proximity sensor 12 is located in a vehicle 14 and senses, in a known manner, the presence of a person adjacent the vehicle 14. The proximity sensor 12 may sense a person touching a vehicle door handle, or sense an attempt to actuate a door handle which activates a switch. Alternatively, the sensor 12 may comprise a short range proximity sensor located in the vehicle using, for example, capacitive monitoring to sense the presence of a person adjacent the vehicle. When the proximity sensor 12 is activated, it causes a vehicle transponder 16 in the vehicle 14 to transmit a radio frequency trigger signal at a predetermined, fixed carrier frequency. This trigger signal includes a random number generated by random number generator 17 associated with the transponder 16. The trigger signal also incorporates coded vehicle identification information that uniquely identifies the vehicle 14. The trigger signal may be transmitted a predetermined number of times, or over a predetermined period, following activation of the proximity sensor. Alternatively, one trigger signal may be transmitted for each

proximity sensor activation.

The random number generated by the generator 17 is used to establish one or more frequencies to which the transponder receiver 26 in the vehicle is to be tuned to receive a response to the transmitted trigger signal. In this embodiment, the RF frequencies may vary between 200 MHz and 400MHz, although it will be appreciated that a broader or different bandwidth may be used.

At least one electronic identification device 18 is associated with the vehicle transponder 16. The device 18 has receiver and decoder circuitry 19 to receive and decode a received signal, a processor 21 and a transmitter 24. A unique identification number together with vehicle identification information is held in a store 23, and the processor is programmed to conduct calculations in accordance with an algorithm 22.

If the person sensed by the proximity sensor 12 is carrying an electronic identification device 18, the device receives the trigger signal in the receiver and decoder circuitry 19 and determines if the transmitted coded vehicle identification information matches the stored vehicle information in the device. If the received and stored information matches, the random number included with the trigger signal is manipulated in processor 21 using an algorithm 22 and the stored unique number in the store 23. The processor thereby generates a resulting response signal that comprises one or more bursts of RF energy of given duration and at one or more frequencies, the three variables (number of pulses generated, their duration and the RF frequencies of the pulses) being determined by the algorithm working with the unique stored number in conjunction with the random number transmitted from the vehicle 14. The response signal is transmitted by the transmitter 24 and received by a receiver 26 associated with the transponder 16 in the vehicle 14.

As indicated above, in generating and transmitting the trigger signal, which carries the random number, the receiver 26 in the vehicle is tuned to the frequencies of the expected response signal in accordance with the transmitted random number. On receipt of a response signal of the appropriate frequency or frequencies, a comparator 27 compares the response signal with the expected signal, it being understood that the transponder stores the unique identification number of the device and is able to use the same algorithm to calculate the expected response. If the received response signal matches the expected response, a signal is sent to a door lock actuator 28 to unlock the vehicle door(s).

If vehicle operation authentication is also required of the system, the information exchange described above is repeated when the operator attempts to start the vehicle. In this instance, it is desirable for the system to determine if the identification device 18 is inside the vehicle 14. Accordingly, the power of the trigger signal transmitted by the transponder for this function is controlled so that it is unlikely that the identification device 18 could detect the signal from outside the vehicle. This ensures that the vehicle cannot be operated unless the identification device is within the vehicle. If desired, the system may be designed such that the identification device must be mounted in an appropriate receptacle in the vehicle before the vehicle is able to be started.

It will be appreciated that the security system of the described embodiment is more secure than the previous systems of a similar type as described herein by reason of the use of a variable signal frequency within a wide bandwidth for the response signal. Further, by using an algorithm together with an unique identification number to manipulate the transmitted random number and generate a response signal having at least three variables, vis, the number of pulses, the duration of the pulses and the RF frequencies of the

individual pulses, it will be very difficult to attack the system by the use of normal, portable transceivers.

It will be appreciated that the response signal may also include other variables, such as a polling identification number, the polling of which is determined by the random number.

A security system of the invention may be made substantially more immune to interfering external RF sources than currently known systems by the use of the variable frequency of the response signal. If access to a vehicle is blocked because of an interfering RF signal source, re-activation of the trigger signal will generally give rise to a response signal having a frequency that is not interfered with by the RF source. However, some redundancy should be made in the identification device's response coding to allow for masking which may occur due to interfering external signals at spot frequencies.

It will be appreciated that the principals of this invention may be used in a large number of different applications, such as security access associated with buildings, including external doors, internal doors, lifts, maintenance areas and the like. The principals may also be used to provide authorisation for activities other than access. Thus, the system may be designed to permit only authorised use of equipment

CLAIMS:

1. A security system having transponder means adapted to be actuated to generate and transmit an electromagnetic trigger signal, and a portable electronic device adapted to receive and respond to said trigger signal by transmitting a response signal, the receipt and authentication of which by the transponder means gives rise to a predetermined event, said response signal comprising one or more radio frequency signals of a frequency and duration determined by an algorithm together with a unique number stored in the device and with reference to a random number contained in the trigger signal.

2. A security system according to claim 1 wherein said response signal contains three variables comprising the number of pluses in the RF signal, the frequency of the pulses and the pulse duration.

3. A security system according to claim 1 or claim 2 wherein the transponder means includes a receiver which is tuned to the expected frequency of the response signal in accordance with the random number contained in the trigger signal.

4. A security system according to any one of claims 1 to 3 wherein the transponder means is actuated by a proximity sensor.

5. A security system according to any one of claims 1 to 3 wherein the transponder means is actuated by a switch.

6. A security system according to any one of the preceding claims wherein

the predetermined event is the actuation of a door lock or the enabling of a control system.

7. A security system according to any one of the preceding claims wherein a random number generator is associated with the transponder means and generates a new random number upon each actuation of the transponder means.

8. A security system according to any one of the preceding claims wherein the transponder means transmits the trigger signal for a predetermined period following actuation or until reception of an authenticated response signal.

9. A security system according to any one of the preceding claims wherein said trigger signal incorporates coded identification information that uniquely identifies the transponder

10. A security system according to claim 9 wherein the device stores identification information and on reception of a trigger signal, determines if the transmitted coded identification information match the stored information and generates a response signal only if the information matches.

11. A security system according to any one of the preceding claims wherein the frequency of the response signal varies with each transmission within the range 200 MHz and 400 MHz.

12. A security system according to any one of the preceding claims wherein the frequency of individual pulses of the response signal vary within a predetermined range.

13. A security system according to any one of the preceding claims wherein said transponder means is mounted in a motor vehicle and is actuated by a proximity sensor or a switch associated with a vehicle door handle.

14. A security system according to claim 13 wherein the or a second transponder means is associated with vehicle electrical circuits which are enabled on receipt of an authenticated response signal following transmission of a coded trigger signal initiated by vehicle starting procedures.

15. A security system according to claim 14 wherein the signal strength of the coded trigger signal transmitted on actuation of vehicle starting procedures is such that the signal is unable to be detected by the device outside the vehicle.

16. A security system according to any one of claims 13 to 15 wherein the vehicle includes a receptacle with which the device must be engaged before vehicle electrical systems are able to be enabled.

17. A security system substantially as hereinbefore described with reference to the accompanying drawings.

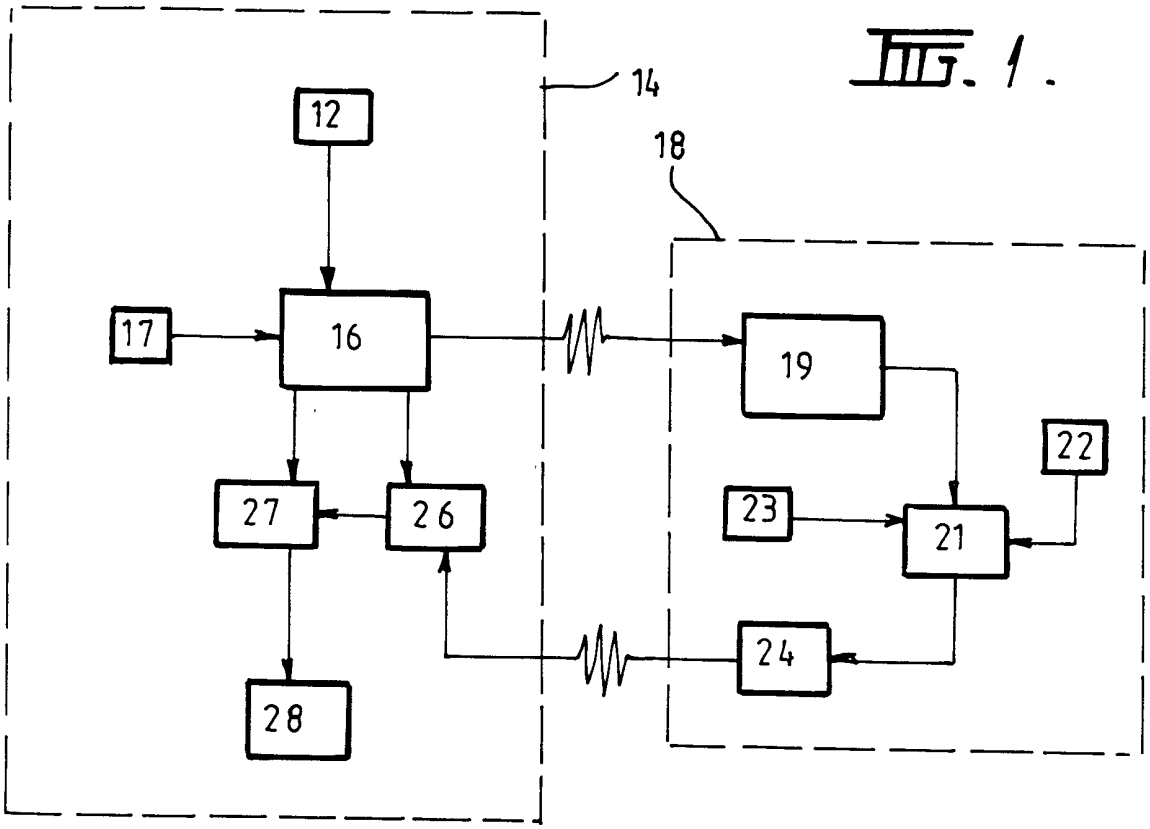


FIG. 1.

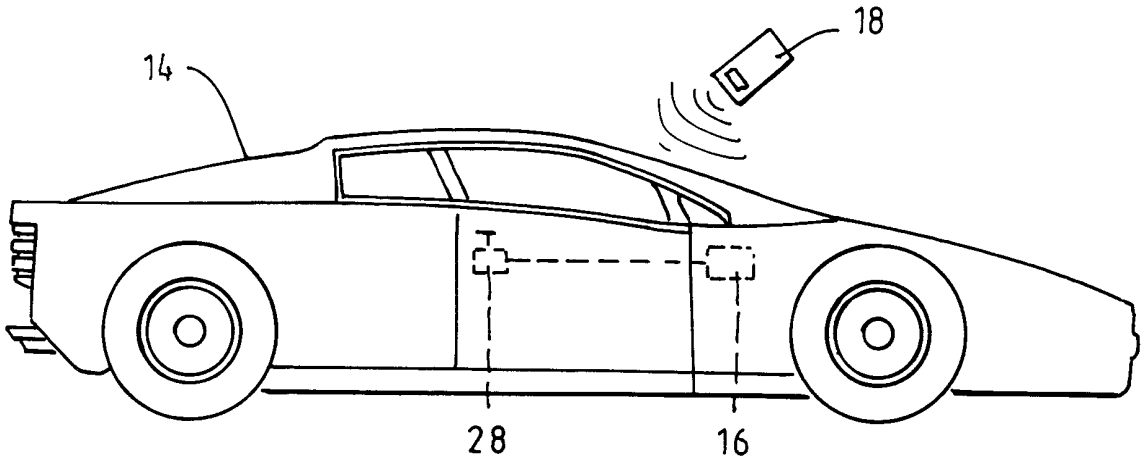


FIG. 2.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU00/01186

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: B60R 25/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: B60R-025/--

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT: B60R-025/IC AND transponder

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP-0926021-A2 (ROVER GROUP LIMITED) 30 June 1999 See abstract and claims.	
A	US-5889471-A (GLEHR et al.) 30 March 1999 See abstract and claims.	
A	US-5790014-A (CAMPBELL et al.) 4 August 1998 See abstract and claims.	

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 January 2000	1 - DEC 2000
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **MICHAEL HARDY** Telephone No : (02) 6283 2547

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU00/01186

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE-19637387-C1 (SIEMENS AG) 29 January 1998 See abstract.	
A	FR-2717327-A1 (VALEO ELECTRONIQUE) 15 September 1995 See abstract and claims.	
A	US-4738334-A (WEISHAUPT) 19 April 1988 See abstract and claims.	

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU00/01186

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
EP	926021	GB	2332548				
US	5889471	EP	730071				
US	5790014	CA	2232256	EP	874439	JP	11046157
DE	19637387	NONE					
FR	2717327	NONE					
US	4738334	DE	3536377	EP	218251		

END OF ANNEX