

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
17 August 2006 (17.08.2006)

PCT

(10) International Publication Number
WO 2006/085246 A1

(51) International Patent Classification:
H04B 1/38 (2006.01) **H04B 5/00** (2006.01)

(21) International Application Number:
PCT/IB2006/050351

(22) International Filing Date: 2 February 2006 (02.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
05300106.1 9 February 2005 (09.02.2005) EP

(71) Applicant (for all designated States except US): **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **MAUGARS, Philippe** [FR/FR]; C/o Triester Strasse 64, A-1101 Vienna (AT). **GAMAND, Patrice** [FR/FR]; C/o Triester Strasse 64, A-1101 Vienna (AT).

(74) Agents: **RÖGGLA, Harald** et al.; Philips Intellectual Property & Standards, Triester Strasse 64, A-1101 Vienna (AT).

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

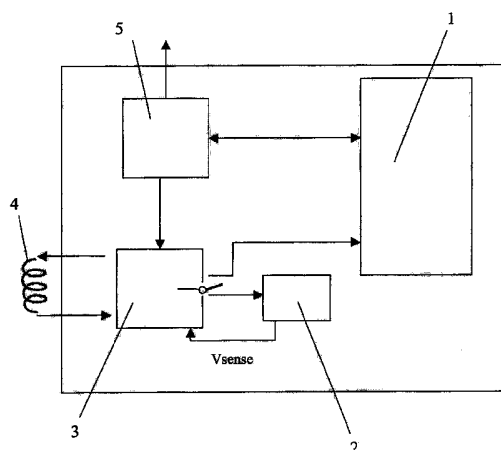
(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT,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

Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

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.

(54) Title: METHOD FOR ENSURING A SECURE NFC FUNCTIONALITY OF A WIRELESS MOBILE COMMUNICATION DEVICE AND WIRELESS MOBILE COMMUNICATION DEVICE HAVING A SECURE NFC FUNCTIONALITY



(57) Abstract: The invention provides a method for ensuring a secure NFC functionality of a wireless mobile communication device comprising the steps of detecting the charge state of a first energy source (1) which supplies the voltage for operating the wireless mobile communication device (S1); switching off the first energy source and switching on a second energy source (2), if the detected charge state of the first energy source (1) falls below a threshold (S2); detecting the charge state of the second energy source (2), if an external NFC signal is received (S3); charging of the second energy source via voltage induced by a received NFC signal to allow at least one secure NFC transaction, if the detected charge state of the second energy source (2) is below a threshold (S4). Furthermore the invention provides a wireless mobile communication device having a secure NFC functionality, which is always ready for operation of at least the secure NFC functionality.

Method for ensuring a secure NFC functionality of a wireless mobile communication device
and wireless mobile communication device having a secure NFC functionality

5

FIELD OF THE INVENTION

The invention relates to a method for ensuring a NFC functionality of a wireless mobile communication device.

The invention also relates to a wireless mobile communication device having a
10 secure NFC functionality operated by such a method.

BACKGROUND OF THE INVENTION

Involving from a combination of contactless identification and networking technologies, near field communication (NFC) is a wireless connectivity technology that
15 enables convenient short-range communication between electronic devices. NFC is a very short-range wireless technology, for distances measured in centimeters, and is optimized for intuitive, easy and secure communication between various devices without user configuration. In order to make two devices communicate, users bring them close together or even make them touch. The devices' NFC interfaces will automatically connect and configure
20 themselves to form a peer to peer network.

A further application of NFC is the combination of NFC applications with smart card security concept so that devices act like contactless smart card with cryptographic capabilities. This NFC technology can be denoted as secure NFC and is standardized in ISO 18092, ECMA 340 and ECGS 102190. NFC is also compatible to the broadly
25 established contactless smart card infrastructure based on ISO 14443A.

The secure NFC can be included in wireless mobile communication devices like mobile phones, PDAs and the like. This means that confidential data and data that represents values is stored in a secure memory area and always stays on the mobile communication device. An authentication is performed by the secure NFC functionality included, for
30 example, in a PDA or mobile phone and transmitted data can be encrypted by the secure NFC functionality using a private encryption key stored on the mobile phone.

The implementation of the secure NFC functionality into a wireless mobile communication device like a mobile phone allows the application of the mobile phone as for example a virtual stored transport ticket or an access key to a building (home or office),

wherein the ticket or the access key is transferred by the secure NFC functionality of the mobile phone for granting the access to a transport means or a building.

However, wireless mobile communication devices have to be equipped with autonomous energy sources due to their mobile character. Such energy sources are usually batteries or accumulators, which can be recharged. Hence, it is conceivable that the readiness of operation of the wireless mobile communication device is not always guaranteed as the battery or the accumulator is unloaded by the time. Therefore, it is possible that the NFC functionality of the mobile phone is not available if needed. This, of course, creates problems for a user when he needs to transfer ticket data or access data via secure NFC in order to get an access to a building, a train or train station, a laboratory room, etc.

OBJECT AND SUMMARY OF THE INVENTION

It is an object of the invention to provide a method defined in the first paragraph and a wireless mobile communication device as defined in the second paragraph, in which the disadvantages defined above are avoided.

In order to achieve the object defined above with a method for ensuring a secure NFC functionality of a wireless mobile communication device according to the invention characteristic features are provided so that a system according to the invention is characterized defined below that is:

Method for ensuring a NFC functionality of a wireless mobile communication device comprising the steps of
detecting the charge state of a first energy source which supplies the voltage for operating the wireless mobile communication device;
switching off the first energy source and switching on a second energy source, if the detected charge state of the first energy source falls below a threshold;
detecting the charge state of the second energy source, if an external NFC signal is received;
and
charging of the second energy source via voltage induced by a received NFC signal to allow at least one NFC transaction, if the detected charge state of the second energy source is below a threshold.

In order to achieve the object defined above with a wireless mobile communication device having secure NFC functionality according to the invention characteristic features are provided so that a device according to the invention can be characterized in the way defined below that is:

Wireless mobile communication device having a NFC functionality comprising antenna means adapted to receive and send NFC signals;
an NFC circuit adapted to provide a secure NFC functionality for the wireless mobile communication device;

- 5 a first energy source adapted to supply power for the wireless mobile communication device;
a second energy source connectable to the NFC circuit to supply power thereto;
control means adapted to monitor the charge state of the first energy source and adapted to switch off the first energy source and to switch on to the second energy source if the monitored charge state of the first energy source falls below a threshold;
10 detecting means adapted to detect the charge state of the second energy source; and
wherein the second energy source is adapted to be charged via voltage induced by an external NFC signal received by the antenna means if the detected charge state the second energy source is not sufficient to allow at least one NFC transaction.

The characteristic features according to the invention provide the advantage that
15 a wireless mobile communication device having NFC functionality is always ready to operate with respect to at least the NFC functionality. Hence, the method of operating a wireless mobile communication device having a NFC functionality and the wireless mobile communication device broadens the application scope of wireless mobile communication devices to areas with security or control demands such as ticket control systems or room
20 access systems.

The measures as claimed in claim 2 and claim 5 provide the advantage of an additionally loading of the main power supply of the wireless mobile communication device while performing a NFC transaction.

The measures as claimed in claim 3 provides the advantage of an enhanced
25 operational readiness of the wireless mobile communication device with respect to the secure NFC functionality.

The measures as claimed in claim 6 provide the advantage of an fast achievable ready to use state of the wireless mobile communication device with respect to the (secure) NFC functionality.

30 The measures as claimed in claim 7 provide the advantage of an effective implementation of the second energy source, which can be manufactured at low costs.

The aspects defined above and further aspects of the invention are apparent from the examples of embodiment to be described hereinafter and are explained with reference to the examples to embodiment. The invention will be described in more detail hereinafter with

reference to the examples of embodiment but to which the invention is not limited.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows the basic concept of the invention in form of a schematic flow
5 diagram.

Fig. 2 shows a wireless mobile communication device according to an
embodiment to the invention in form of a block diagram.

DESCRIPTION OF EMBODIMENTS

10 It has to be appreciated that if, in connection with this invention, it is referred to NFC, any short-range wireless communication technology is encompassed which is not necessarily using the standardized NFC. Hence, the secure NFC functionality according to this invention is to be understood to encompass various protocols and ID types and not only RFID.

15 Referring to Fig. 1, a method for ensuring a secure NFC functionality of a wireless mobile communication device according to a first embodiment is described. The method starts with the step S1 of detecting the charge state of a first energy source 1 with supplies the voltage for operating the wireless mobile communication device. The detecting could be included in a monitoring of the first energy source, which could be performed by a
20 power management unit (PMU). The detected charge state of the first energy source (1), for example a main battery, is then compared with a predetermined threshold.

If the detected charge state of the first energy source 1 falls below a threshold, then the first energy source 1 is switched off. The threshold is preferably defined as a charge state value of the main battery, which is not able to maintain the overall operation of the
25 wireless mobile communication device. However, the threshold could also be defined according to a stand-by condition. In addition, after switching off the first energy source, a second energy source 2 is switched on for maintaining at least the NFC functionality of the wireless mobile communication device. This switching step is denoted with S2.

If the wireless mobile communication device having a secure NFC functionality
30 receives an external NFC signal, for example, a request of a RFID reader to send an ID, the charge state of the second energy source 2 is detected. This step is denoted with S3.

If the detected charge state of the second energy source 2 is below a threshold the second energy source (2) is charged via a voltage induced by the external NFC signal. The threshold is preferably defined as a charge state value necessary for allowing at least one

NFC transaction to answer the NFC signal. However, the threshold could also set to a value that corresponds to more than one NFC transaction. A NFC transaction within the meaning of the invention is at least a pair of an external NFC signal and a corresponding NFC answer signal of the device. The charging step is denoted with S4.

5 By this method the secure NFC functionality can be ensured or maintained even if the first energy source with the necessary operating voltage has been discharged as the power supply of the device is switched to a second energy source which supplies at least the NFC circuit of the device with power. Since the second energy source need not to be charged beforehand as it can be charged by the voltage induced by an external NFC signal initiating a
10 NFC transaction, the NFC functionality is always available even if the second energy source has been discharged over the time, for example by a leak current, and the first energy source is switched off because of a discharged state. Hence, the NFC functionality of the wireless mobile communication is always ensured and no unexpected problems are created for a user if he needs to use the secure NFC functionality of the wireless mobile communication device.

15 The method can be advantageously extended in that way that the step of charging the second energy source 2 is continued even, if the second energy source 2 is completely loaded, by switching the charging operation from the second energy source to the first energy source which is then at least partially reloaded via the voltage induced by a NFC signal received by the wireless mobile communication device. For example in a case, where
20 the user of a wireless communication device having a secure NFC functionality which allows him access to a secure area of a building, the user is able to get access to the house since the secure NFC functionality is maintained even if the main battery (i.e. first energy source) of the wireless mobile communication device has been switched off because of a too low charge state. However, the user is not only granted access to the building by just bringing his
25 wireless mobile device in the vicinity (i.e. the near field) of a RFID reader and initiating a NFC transaction but he can also at least partially reload the main battery of the wireless mobile communication device as long as he remains in the receiving range of the RFID reader signal. Of course, as the energy density of the NFC signal can not be made too high in order not too harm the health of the user, a complete reloading of the main battery will take a
30 long time compared with the quick charging of the second energy source.

 It has to be appreciated that the method of the invention is not limited to RFID readers and RFID signals since almost every kind of energy-bearing signal can be used for a short-range communication as long as the wireless mobile communication device is adapted to use the received energy for charging the second energy source.

Referring to Fig. 2, an embodiment of a wireless mobile communication device having a secure NFC functionality according to the invention is illustrated in form of a block diagram. The wireless mobile communication device comprises a first energy source 1 which can be any usual battery or accumulator. In this embodiment, the first energy source 1 is a rechargeable main battery, which supplies the operating voltage for all components wireless mobile communication device including a NFC circuit 3, which provides the NFC functionality. The wireless mobile communication device further comprises antenna means 4 for receiving and sending NFC signals. NFC signals to be sent are generated in the NFC circuit 3 and external NFC signals like RFID requests are received by the antenna means and forwarded to the NFC circuit. The NFC circuit of this embodiment is adapted for RFID signals; however, other signal protocols could be used as well.

The wireless mobile communication device further comprises control means 5 which are adapted to detect the charge state of the main battery 1. Furthermore, the control means are adapted to control distribution of the operating voltage supplied by the main battery to the NFC circuit as well as to the other components of the wireless mobile communication device. In this embodiment, the control means are embodied as a power management unit (PMU) chip.

The wireless mobile communication device further comprises a second energy source 2, which is connectable to the NFC circuit 3 by switching means to supply power to the NFC circuit 3 for performing the secure NFC functionality. The second energy source 2 is preferably an integrated micro battery and can be realized on the passive companion chip of the NFC circuit also used for antenna adaptation and supply decoupling. Preferably, the integrated micro battery is embedded with an integrated silicon technology as PICS technology for instance. This battery technology by solid-state electrolyte deposition in silicon for the integrated micro battery can be manufactured by very low additional costs when using trench capacitive process as in PICS process.

In a preferred embodiment, the micro battery can be charged at the time of power up of the wireless mobile communication device so that the secure NFC functionality is immediately available if the main battery is switched off due to a too low charge state or operation voltage, respectively.

However, if the integrated micro battery is not loaded, the micro battery is adapted to be charged by a current that is delivered by the NFC circuit according to a voltage induced by a received NFC signal. As an integrated micro battery can be charged in a very short time, the delay in receiving the RFID signal request and answering it will be almost

unnoticeable for the user.

Detection of the charge state of the integrated micro battery can be either achieved by the control means 5 which are for example a power management unit (PMU) or with the NFC circuit 3. In this embodiment, the charge state of the integrated micro-battery 2 can be detected via a detection line signal Vsense connected to the NFC circuit 3.

The wireless mobile communication device having a secure NFC functionality according to this embodiment is always ready for operation with respect to the secure NFC functionality even if the main battery 1 has been switched off and the integrated micro battery 2 is not sufficiently charged.

In a further embodiment of the wireless communication device according to the invention, switching means are provided, preferably integrated in the NFC circuit 3, which enables the main battery 1 to be charged by voltage induced by received NFC signals for reloading if switched off due to a too low charge state. However, a complete reload of the main battery takes a very long time as the capacity of the main battery 1 is much higher than the capacity of the integrated micro battery and the energy density of the NFC signal is rather low as mentioned above. Since a RFID transaction needs approximately 100 mA/200 ms, the capacity of the micro battery 2 need not to be as big as the capacity of the main battery since it only supplies the NFC circuit with power. Furthermore, a micro battery preferably has a very fast recharging characteristic so as to not cause any noticeable delay in performing a NFC transaction.

It has to be appreciated that the concept of the invention can also be applied to other protocols than NFC. For example, a short message transmission via GSM protocol is also conceivable. In fact, any short-range communication protocol which is able to deliver a energy-bearing signal sufficient for inducing a voltage that is able to be used for charging the second energy source up to a level which allows at least one secure NFC transaction can be used. The term NFC therefore has not to be interpreted to limit the scope of the claims to the NFC standard functionality as such, but for all kind of RFID functionalities for networking technologies.

It has to be appreciated that the reference signs within the claims are only given for illustrative purpose and shall not be construed as limiting the scope of the method for which protection is sought after.

CLAIMS

1. Method for ensuring a NFC functionality of a wireless mobile communication device comprising the steps of
detecting the charge state of a first energy source (1) which supplies the voltage for operating
5 the wireless mobile communication device (S1);
switching off the first energy source and switching on a second energy source (2), if the
detected charge state of the first energy source (1) falls below a threshold (S2);
detecting the charge state of the second energy source (2), if an external NFC signal is
received (S3); and
10 charging of the second energy source via voltage induced by a received NFC signal to allow
at least one NFC transaction, if the detected charge state of the second energy source (2) is
below a threshold (S4).
2. Method according to claim 1, the step of charging further comprises charging
15 of the first energy source via the voltage induced by the external NFC signal as long as an
external NFC signal is received if the second energy source is completely loaded.
3. Method according to claim 1 or 2, further comprising pre-charging of the
second energy source at the time of power-up of the wireless mobile communication device
20 so as to allow at least one NFC transaction if the first energy source (1) has been switched off
without charging the second energy source (2) via voltage induced by a NFC signal.
4. Wireless mobile communication device having a NFC functionality
comprising
25 antenna means (4) adapted to receive and send NFC signals;
a NFC circuit (3) adapted to provide a NFC functionality for the wireless mobile
communication device;
a first energy source (1) adapted to supply power for the wireless mobile communication
device;
30 a second energy source (2) connectable to the NFC circuit (3) to supply power thereto;

control means (5) adapted to monitor the charge state of the first energy source (1) and adapted to switch off the first energy source (1) and to switch on to the second energy source (2) if the monitored charge state of the first energy source (1) falls below a threshold; detecting means adapted to detect the charge state of the second energy source (2); and
5 wherein the second energy source (2) is adapted to be charged via voltage induced by an external NFC signal received by the antenna means (4) if the detected charge state the second energy source (2) is not sufficient to allow at least one NFC transaction.

5. Wireless mobile communication device according to claim 4 further
10 comprising switching means to switch the charging operation via voltage induced by an external NFC signal from the second energy source (2) to the first energy source (1) if the second energy source (2) is completely loaded.

6. Wireless mobile communication device according to claims 4 or 5 wherein the
15 second energy source (2) is faster chargeable than the first energy source (1).

7. Wireless mobile communication device according to any of the claims 4 to 6 wherein the second energy source (2) is an integrated micro battery.

1/2

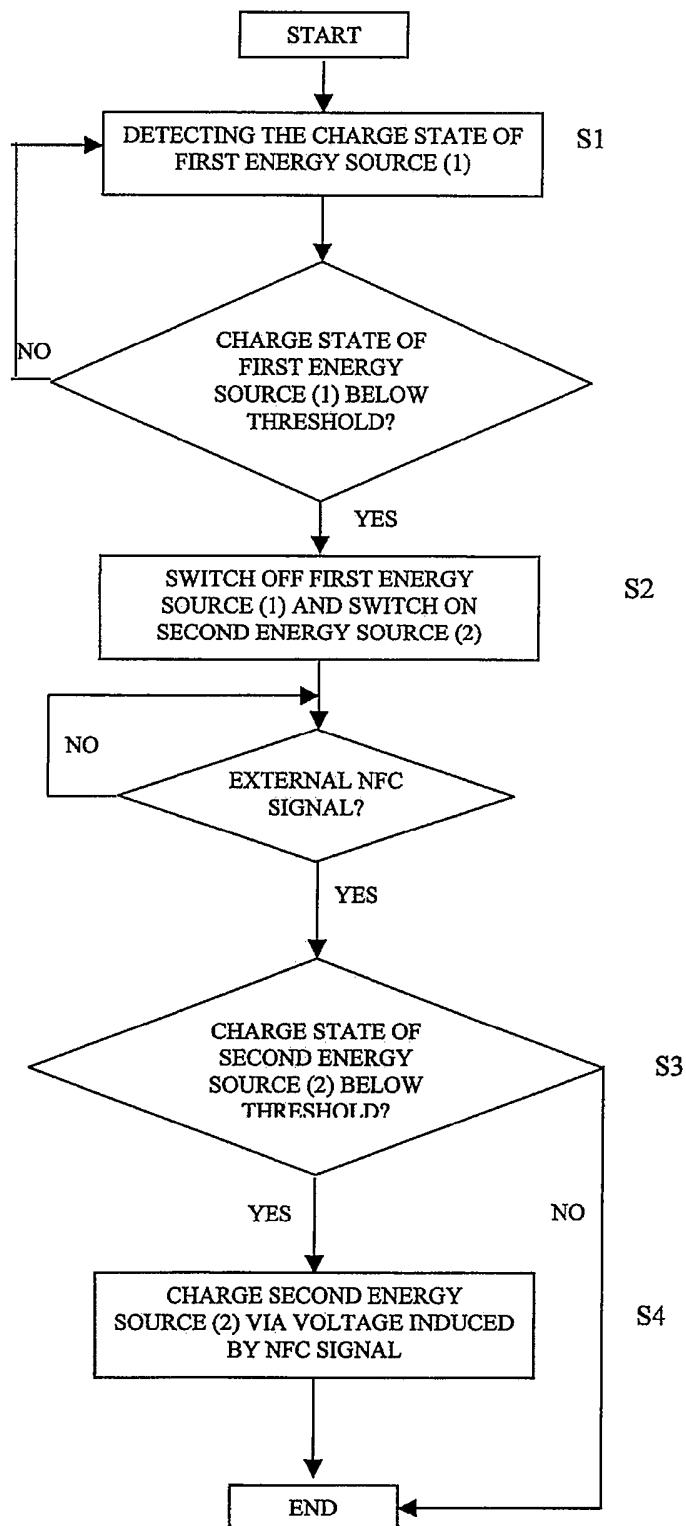


Fig.1

2/2

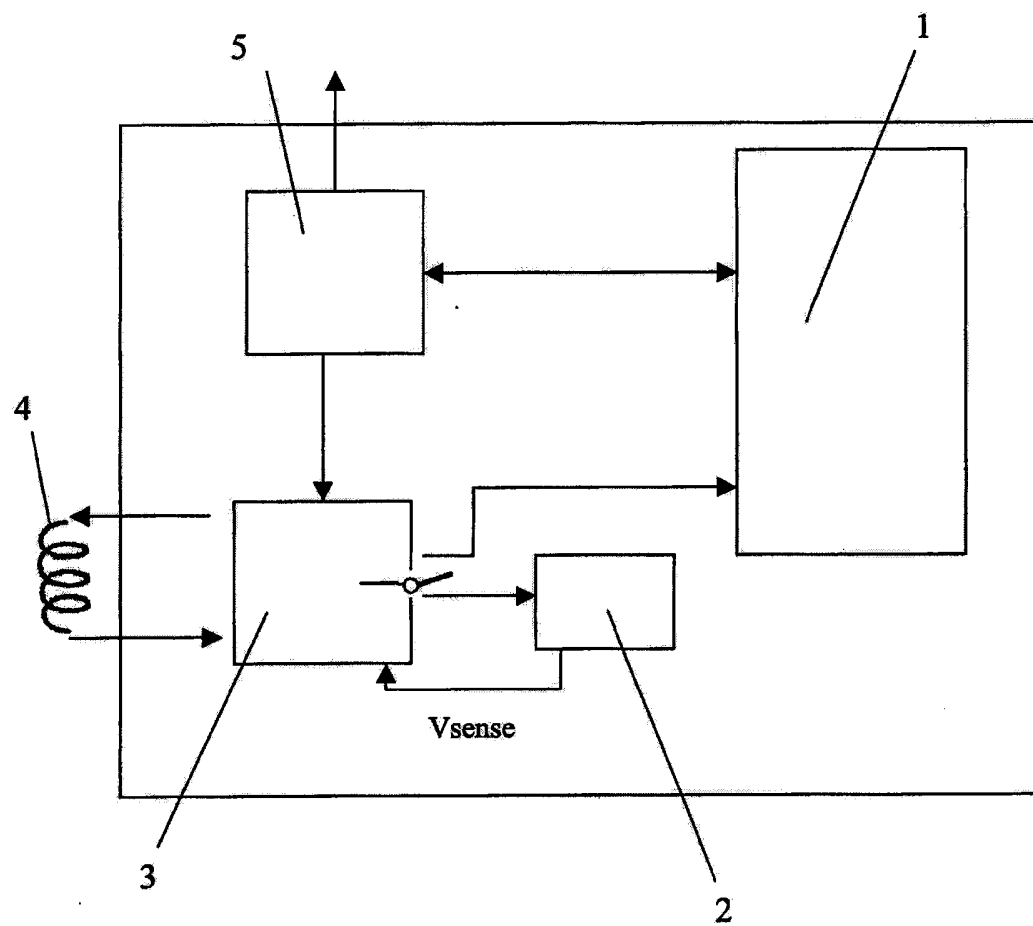


Fig.2

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2006/050351

A. CLASSIFICATION OF SUBJECT MATTER

INV. H04B1/38

ADD. H04B5/00

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)

H04B G06K H04M

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 practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/146821 A1 (BRANDT JAN) 7 August 2003 (2003-08-07) paragraph [0014] - paragraph [0018] paragraphs [0024], [0026]; figures 1,2	1,4,6,7
Y	US 4 908 523 A (SNOWDEN ET AL) 13 March 1990 (1990-03-13) column 1, line 9 - line 14 column 4, line 67 - column 5, line 7; figures 1,2	1,4,6,7
Y	WO 00/41334 A (MOTOROLA INC) 13 July 2000 (2000-07-13) page 15, line 6 - line 30 page 21, line 4 - page 22, line 29 page 25, line 18 - page 26, line 34; figures 4,7,10	1,4,6,7
	----- -/--	

☒ Further documents are listed in the continuation of Box C.☒ 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 document 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

21 June 2006

Date of mailing of the international search report

05/07/2006

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sinapius, G

INTERNATIONAL SEARCH REPORT

International application No

PCT/IB2006/050351

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002/041175 A1 (LAUPER ERIC ET AL) 11 April 2002 (2002-04-11) paragraph [0016] - paragraph [0020] paragraph [0028]; figures 1,2 -----	1,4

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2006/050351

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2003146821	A1	07-08-2003	AU 2003205931 A1 EP 1474785 A1 WO 03067539 A1	02-09-2003 10-11-2004 14-08-2003
US 4908523	A	13-03-1990	NONE	
WO 0041334	A	13-07-2000	AU 2214100 A	24-07-2000
US 2002041175	A1	11-04-2002	AU 4128899 A WO 0079771 A1 EP 1186150 A1	09-01-2001 28-12-2000 13-03-2002