(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 085 481 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
08.02.2012 Bulletin 2012/06

(51) Int Cl.:
G08C 19/28 *(2006.01)* ***G07C 9/00*** *(2006.01)*

(21) Application number: **00650129.0**

(22) Date of filing: **13.09.2000**

(54) **A remote control transmitter**

Ein Fernsteuersender

Un émetteur de télécommande

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **13.09.1999 IE 990766**

(43) Date of publication of application:
21.03.2001 Bulletin 2001/12

(73) Proprietor: **FAAC Electronics Limited**
Dublin 24 (IE)

(72) Inventors:
- **Moriarty, Donal**
  Clondalkin,
  Dublin 22 (IE)
- **O'Connell, Thomas**
  Blackrock,
  County Dublin (IE)

(74) Representative: **Weldon, Michael James et al**
John A. O'Brien & Associates
Third Floor,
Duncairn House,
14 Carysfort Avenue
Blackrock, Co. Dublin (IE)

(56) References cited:
WO-A-96/37063 **WO-A-97/33373**
US-A- 5 661 804 **US-A- 5 767 784**

EP 1 085 481 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The invention relates to a transmitter for a remote control group for a shared function such as opening a garage door. It also relates to a receiver for such a group and to a group of a receiver and a plurality of transmitters.

[0002] Our prior European Patent No. EP0651119B1 describes a transmitter having a capability of learning a code so that it can be used in a remote control group. An embedded instruction allows versatility as to how learning takes place. Also, there is automatic "listening" every time the transmit button is pressed.

[0003] Such features in a transmitter are very helpful for learning. However, there remains a need for improving security in the transmitter-receiver link. One approach to achieving improved security is to encrypt using an encryption key. However, this means that the installation engineer needs to access the receiver to program it to allow introduction of each new transmitter of the group. This is time-consuming and expensive.

[0004] It is therefore an object of the invention to provide:

(a) improved security in the transmitter-receiver link, with

(b) automatic introduction of a new transmitter to the receiver with out the need for installation engineer to be involved.

[0005] US5661804 describes a trainable transceiver for learning and transmitting an activation signal that includes a rolling code.

[0006] According to the invention, there is provided a remote control group as set out in claim 1.

[0007] In one embodiment, the valid code is variable according to pre-set criteria.

[0008] In one embodiment, the valid code comprises a hopping index.

[0009] In another embodiment, the valid code comprises a combination of a fixed discrimination value known to the receiver and a hopping index.

[0010] In one embodiment, the slave transmitter comprises means for generating the encryption key by processing a manufacturer-set key with a site code which is unique to the group.

[0011] In one embodiment, the slave transmitter comprises means for receiving the site code in an encrypted teaching radiation signal and for decrypting said signal to determine the site code using a teaching decryption key.

[0012] In one embodiment, the slave transmitter comprises means for storing a transmitter-specific serial number and for transmitting the serial number together with the encrypted code.

[0013] According to another aspect, the master transmitter processor comprises:

means for storing a site code which is unique to the remote control group,

means for encrypting the site code with a teaching encryption key for teaching; and

means for directing transmission of the encrypted site code in a teaching radiation signal.

[0014] In one embodiment, the receiver processor comprises means for:

identifying a transmitter serial number in a received transmission and determining if it is valid,

identifying a hopping index and a discrimination value in the decrypted code, and

determining if the discrimination value and the hopping index are valid.

[0015] In another embodiment, the receiver processor comprises means for determining if the serial number is valid by:

comparing the serial number with a stored list of valid serial numbers,

determining that the serial number is valid if it is the same as a stored valid serial number or if it subsequently receives a fresh encrypted code containing the same serial number and a valid hopping index.

[0016] The invention will be more clearly understood from the following description of some embodiments thereof, given by way of example only with reference to the accompanying drawings in which Fig. 1 is a schematic diagram of a remote control group transmitter of the invention.

[0017] Referring to Fig. 1, remote control group transmitter 1 comprises:

2: a microprocessor,
3: a memory having a capacity for four site (group) codes, four serial numbers, four hopping indexes, four encryption keys, and four discrimination values,
4: a radiation receiver connected to the microprocessor 2,
5: a transmitter antenna, connected to an oscillator circuit 6,
7: four switches,
8: a battery pack, and
9: a regulator providing + Vreg for all of the circuit.

[0018] The memory capacity is adequate for four sets of data, as described above. This allows the transmitter 1 to be used for up to four different remote control groups. However, for clarity, operation for only one group is de-

scribed below.

[0019] The microprocessor 2 is programmed to recognise a switch 7 depression as a transmit instruction. Simultaneous depression of two or more switches in various pre-set configurations are interpreted as user instructions for auxiliary functions such as a teach mode or randomisation of codes. Programming of the microprocessor 2 at manufacture determines whether the transmitter is a master or a slave. Slaves do not have a teach mode. The transmitter 1 is a slave.

[0020] The transmitter 1 is part of a remote control group also comprising a receiver and a master transmitter. The latter is used for teaching both the receiver and the transmitters 1. It has the same hardware configuration as the transmitter 1, but is additionally programmed with a teach mode.

[0021] The remote control group is given a unique site code by the installer and the master transmitter teaches the site code to the receiver and to the transmitters 1. This effectively empowers the installer to set the manner in which the remote control group operates from a security viewpoint. Each master transmitter is pre-programmed at manufacture with a unique (to it) site code. Therefore the installer may use the pre-programmed site code of a master transmitter as that of the group. Alternatively, he may change it by randomising the pre-set value.

[0022] Each new transmitter stores the following after manufacture:

a 24-bit serial number (pre-programmed at manufacture) which is unique to the new transmitter,

an initial 20-bit hopping index which will subsequently be incremented every time the new transmitter is used,

a manufacturer-set encryption key, and

a decryption key for decrypting a site code in a teaching session.

[0023] The master transmitter teaches the site code to a (slave) transmitter 1 using a teaching encryption key. The transmitter 1 decrypts it using a teaching decryption key. After decryption, the transmitter 1 uses the site code to generate the encryption key for use in sending signals to the receiver for control of the shared group function. After it is used to generate the encryption key, it is not necessarily stored as it is not required again. The encryption key is 64 bits long. The master transmitter also teaches a discrimination value to the transmitter 1. This is an agreed value that enables the receiver to determine that it has correctly decrypted the transmission. It could, for example, be part of the site code or the serial number or any other agreed number.

[0024] The encryption key could alternatively be generated by only the master transmitter and taught to the receiver and the transmitters 1. However this suffers from the disadvantage of involving transmission of the encryption key.

[0025] When the user is given the new transmitter, he or she can immediately use it without the need for an installation engineer to access the receiver. There are two stages to the introduction of the new transmitter to the receiver by the user as follows.

(a) Initial Acceptance

[0026] The user presses the "transmit" button. The microcontroller encrypts the initial hopping index and the discrimination value with the encryption key to provide a valid encrypted code. The (unencrypted) serial number and the encrypted code are transmitted, and are received by the receiver. The receiver decrypts the code using its stored decryption key to determine the discrimination value and the initial hopping index. The receiver then checks the (decrypted) discrimination value and, if valid, it stores the serial number and the initial hopping index.

(b) Acceptance and Activation

[0027] The user presses the "transmit" button again and the transmitter increments the hopping index and then encrypts the discrimination value and the incremented hopping index to provide a new encrypted code. Although there may only be a one-digit difference between this incremented hopping index and the initial hopping index, the encrypted code is very different due to the complex nature of the encryption. The receiver decrypts the new encrypted code to determine the discrimination value and the incremented hopping index, and reads the serial number. If the following criteria are met the receiver activates the shared group function (e.g. opens a gate) and stores the incremented hopping index:

the serial number is the same as the first one,
the decrypted incremented hopping index matches the hopping criterion (greater than the first one), and
the discrimination value is correct.

[0028] Thereafter, the user only needs to press the transmit button once to activate the shared group function. This two-stage acceptance process prevents a spuriously "acceptable" noise signal from being able to activate the group function.

[0029] It will be appreciated that there is no need for the installation engineer to program the receiver to introduce (validate) a new transmitter. However, this is not achieved at the expense of reduced security as there is comprehensive encryption. Thus, for example, an installer organisation may teach a new transmitter and send it to the user in the post, with considerable savings in time and money. Another aspect contributing to security is the fact that "breaking" of encryption in one group will have no effect on security at another group having the same

or another manufacturer's equipment. This is because the encryption key is unique to each group. Also, unauthorised copying of the transmitted encrypted code is of no benefit to a thief as it changes from one transmission to the next in an unpredictable manner due to encryption of the combined discrimination value and incrementing hopping index. It is envisaged that where particularly strong security is required (such as at a bank) the user may safely store the (single) master transmitter thus preventing any unauthorised teaching of new transmitters.

[0030] The invention is not limited to the embodiments described but may be varied in construction and detail.

Claims

1. A remote control group for a site, the group comprising:

at least one slave transmitter comprising a transmitting device, a user transmit button, a processor, a radiation receiver and a memory,
a master transmitter for teaching the slave transmitter, the master transmitter comprising a memory, a processor, and a transmit device, and
a receiver comprising a memory, an interface to a shared function, and a processor comprising means for controlling the shared function via said interface,
wherein each slave transmitter processor comprises means for encrypting a valid code with an encryption key to generate an encrypted code, and directing transmission of the encrypted code, and
wherein the receiver processor comprises means for decrypting a received encrypted code to generate a decrypted code, and for determining if the decrypted code is valid,
characterised in that,
the encryption key used by each slave transmitter processor to encrypt the valid code is uniquely associated with the remote control group, and each slave transmitter comprises means for learning the encryption key in response to a teaching radiation signal transmitted by the master transmitter;
the master transmitter processor comprises means for teaching the encryption key to the slave transmitter and to the receiver; and
the receiver processor comprises means for storing a decryption key uniquely associated with the remote control group, and using said decryption key to decrypt a received encrypted code.

2. A remote control group as claimed in claim 1, wherein the valid code is variable according to pre-set criteria.

3. A remote control group as claimed in claim 2, wherein the valid code comprises a hopping index.

4. A remote control group as claimed in claim 2 or 3, wherein the valid code comprises a combination of a fixed discrimination value known to the receiver and a hopping index.

5. A remote control group as claimed in claim 1, wherein the slave transmitter comprises means for generating the encryption key by processing a manufacturer-set key with a site code which is unique to the group.

6. A remote control group as claimed in claim 5, wherein the slave transmitter comprises means for receiving the site code in an encrypted teaching radiation signal and for decrypting said signal to determine the site code using a teaching decryption key.

7. A remote control group as claimed in any preceding claim, wherein the slave transmitter comprises means for storing a transmitter-specific serial number and for transmitting the serial number together with the encrypted code.

8. A remote control group as claimed in any preceding claim, wherein the master transmitter processor comprises:

means for storing a site code which is unique to the remote control group,
means for encrypting the site code with a teaching encryption key for teaching; and
means for directing transmission of the encrypted site code in a teaching radiation signal.

9. A remote control group as claimed in any of claims 4 to 8, wherein the receiver processor comprises means for:

identifying a transmitter serial number in a received transmission and determining if it is valid,
identifying a hopping index and a discrimination value in the decrypted code, and
determining if the discrimination value and the hopping index are valid.

10. A remote control group as claimed in claim 9, wherein the receiver processor comprises means for determining if the serial number is valid by:

comparing the serial number with a stored list of valid serial numbers,
determining that the serial number is valid if it is the same as a stored valid serial number or if it subsequently receives a fresh encrypted code containing the same serial number and a valid hopping index.

Patentansprüche

1. Fernsteuergruppe für einen Ort, wobei die Gruppe Folgendes umfasst:

   wenigstens einen Slave-Sender, der ein Sendegerät, eine Benutzersendetaste, einen Prozessor, einen Strahlungsempfänger und einen Speicher umfasst,
   einen Master-Sender zum Anlernen des Slave-Senders, wobei der Master-Sender einen Speicher, einen Prozessor und ein Sendegerät umfasst, und
   einen Empfänger, der einen Speicher, eine Schnittstelle zu einer gemeinsamen Funktion und einen Prozessor mit Mitteln zum Steuern der gemeinsamen Funktion über die genannte Schnittstelle umfasst,
   wobei jeder Slave-Sender-Prozessor Mittel zum Verschlüsseln eines gültigen Codes mit einem Verschlüsselungsschlüssel zum Erzeugen eines verschlüsselten Codes und zum Leiten des Sendens des verschlüsselten Codes umfasst, und
   wobei der Empfängerprozessor Mittel zum Entschlüsseln eines empfangenen verschlüsselten Codes zum Erzeugen eines entschlüsselten Codes und zum Ermitteln umfasst, ob der entschlüsselte Code gültig ist,
   dadurch gekennzeichnet, dass
   der von jedem Slave-Sender-Prozessor zum Verschlüsseln des gültigen Codes verwendete Verschlüsselungsschlüssel eindeutig der Fernsteuergruppe zugeordnet ist und jeder Slave-Sender Mittel zum Erlernen des Verschlüsselungsschlüssels als Reaktion auf ein von dem Master-Sender gesendetes Anlern-Strahlungssignal umfasst;
   der Master-Sender-Prozessor Mittel umfasst, um dem Slave-Sender und dem Empfänger den Verschlüsselungsschlüssel anzulernen; und
   der Empfängerprozessor Mittel zum Speichern eines eindeutig der Fernsteuergruppe zugeordneten Entschlüsselungsschlüssels und zum Verwenden des genannten Entschlüsselungsschlüssels zum Entschlüsseln eines empfangenen verschlüsselten Codes umfasst.

2. Fernsteuergruppe nach Anspruch 1, wobei der gültige Code gemäß voreingestellten Kriterien variabel ist.

3. Fernsteuergruppe nach Anspruch 2, wobei der gültige Code einen Hopping-Index umfasst.

4. Fernsteuergruppe nach Anspruch 2 oder 3, wobei der gültige Code eine Kombination aus einem dem Empfänger bekannten festen Diskriminanzwert und einem Hopping-Index umfasst.

5. Fernsteuergruppe nach Anspruch 1, wobei der Slave-Sender Mittel zum Erzeugen des Verschlüsselungsschlüssels durch Verarbeiten eines vom Hersteller eingestellten Schlüssels mit einem Ortscode umfasst, der der Gruppe eindeutig zugeordnet ist.

6. Fernsteuergruppe nach Anspruch 5, wobei der Slave-Sender Mittel zum Empfangen des Ortscodes in einem verschlüsselten Anlern-Strahlungssignal und zum Entschlüsseln des genannten Signals zum Ermitteln des Ortscodes mit einem Anlern-Entschlüsselungsschlüssel umfasst.

7. Fernsteuergruppe nach einem der vorherigen Ansprüche, wobei der Slave-Sender Mittel zum Speichern einer senderspezifischen Seriennummer und zum Senden der Seriennummer zusammen mit dem verschlüsselten Code umfasst.

8. Fernsteuergruppe nach einem der vorherigen Ansprüche, wobei der Master-Sender-Prozessor Folgendes umfasst:

   Mittel zum Speichern eines Ortscodes, der der Fernsteuergruppe eindeutig zugeordnet ist, und
   Mittel zum Verschlüsseln des Ortscodes mit einem Anlern-Verschlüsselungsschlüssel zum Anlernen; und
   Mittel zum Leiten des Sendens des verschlüsselten Ortscodes in einem Anlern-Strahlungssignal.

9. Fernsteuergruppe nach einem der Ansprüche 4 bis 8, wobei der Empfängerprozessor Mittel umfasst zum:

   Identifizieren einer Senderseriennummer in einer empfangenen Sendung und Ermitteln, ob sie gültig ist,
   Identifizieren eines Hopping-Indexes und eines Diskriminanzwertes in dem entschlüsselten Code, und
   Ermitteln, ob der Diskriminanzwert und der Hopping-Index gültig sind.

10. Fernsteuergruppe nach Anspruch 9, wobei der Empfängerprozessor Mittel zum Ermitteln umfasst, ob die Seriennummer gültig ist, durch:

    Vergleichen der Seriennummer mit einer gespeicherten Liste von gültigen Seriennummern;
    Feststellen, dass die Seriennummer gültig ist, wenn sie dieselbe ist wie eine gespeicherte gültige Seriennummer oder wenn sie nachfolgend einen frischen verschlüsselten Code empfängt, der dieselbe Seriennummer und einen gültigen

Hopping-Index enthält.

Revendications

1. Un groupe de commande à distance pour un site, le groupe comprenant :

   au moins un émetteur esclave comprenant un dispositif d'émission, un bouton d'émission utilisateur, un processeur, un récepteur de rayonnement et
   une mémoire,
   un émetteur maître d'enseignement de l'émetteur esclave, l'émetteur maître comprenant une mémoire, un processeur et un dispositif d'émission, et
   un récepteur comprenant une mémoire, une interface vers une fonction partagée et un processeur comprenant un moyen de commande de la fonction partagée par l'intermédiaire de ladite interface,
   où chaque processeur d'émetteur esclave comprend un moyen de chiffrement d'un code valide avec une clé de chiffrement de façon à générer un code chiffré, et de direction de l'émission du code chiffré, et
   où le processeur récepteur comprend un moyen de déchiffrement d'un code chiffré reçu de façon à générer un code déchiffré, et un moyen de détermination si le code déchiffré est valide,
   caractérisé en ce que,
   la clé de chiffrement utilisée par chaque processeur émetteur esclave pour chiffrer le code valide est associée de manière unique au groupe de commande à distance, et chaque émetteur esclave comprend un moyen d'apprentissage de la clé de chiffrement en réponse à un signal de rayonnement d'enseignement transmis par l'émetteur maître,
   le processeur émetteur maître comprend un moyen d'enseignement de la clé de chiffrement à l'émetteur esclave et au récepteur, et
   le processeur récepteur comprend un moyen de mise en mémoire d'une clé de déchiffrement associée de manière unique au groupe de commande à distance et d'utilisation de ladite clé de déchiffrement pour déchiffrer un code chiffré reçu.

2. Un groupe de commande à distance selon la Revendication 1, où le code valide est variable en fonction de critères prédéfinis.

3. Un groupe de commande à distance selon la Revendication 2, où le code valide comprend un indice de saut.

4. Un groupe de commande à distance selon la Revendication 2 ou 3, où le code valide comprend une combinaison d'une valeur de discrimination fixe connue du récepteur et d'un indice de saut.

5. Un groupe de commande à distance selon la Revendication 1, où l'émetteur esclave comprend un moyen de génération de la clé de chiffrement par le traitement d'une clé définie par le fabricant avec un code de site qui est unique au groupe.

6. Un groupe de commande à distance selon la Revendication 5, où l'émetteur esclave comprend un moyen de réception du code de site dans un signal de rayonnement d'enseignement chiffré et de déchiffrement dudit signal de façon à déterminer le code de site au moyen d'une clé de déchiffrement d'enseignement.

7. Un groupe de commande à distance selon l'une quelconque des Revendications précédentes, où l'émetteur esclave comprend un moyen de mise en mémoire d'un numéro de série spécifique à l'émetteur et de transmission du numéro de série conjointement avec le code chiffré.

8. Un groupe de commande à distance selon l'une quelconque des Revendications précédentes, où le processeur émetteur maître comprend :

   un moyen de mise en mémoire d'un code de site qui est unique au groupe de commande à distance,
   un moyen de chiffrement du code de site avec une clé de chiffrement d'enseignement destinée à un enseignement, et
   un moyen de direction de l'émission du code de site chiffré dans un signal de rayonnement d'enseignement.

9. Un groupe de commande à distance selon l'une quelconque des Revendications 4 à 8, où le processeur récepteur comprend un moyen :

   d'identification d'un numéro de série d'émetteur dans une transmission reçue et de détermination s'il est valide,
   d'identification d'un indice de saut et d'une valeur de discrimination dans le code déchiffré, et de détermination si la valeur de discrimination et l'indice de saut sont valides.

10. Un groupe de commande à distance selon la Revendication 9, où le processeur récepteur comprend un moyen de détermination si le numéro de série est valide par :

    la comparaison du numéro de série à une liste

conservée en mémoire de numéros de série valides,
la détermination que le numéro de série est valide s'il est identique à un numéro de série valide conservé en mémoire ou s'il reçoit ultérieurement un nouveau code chiffré contenant le même numéro de série et un indice de saut valide.

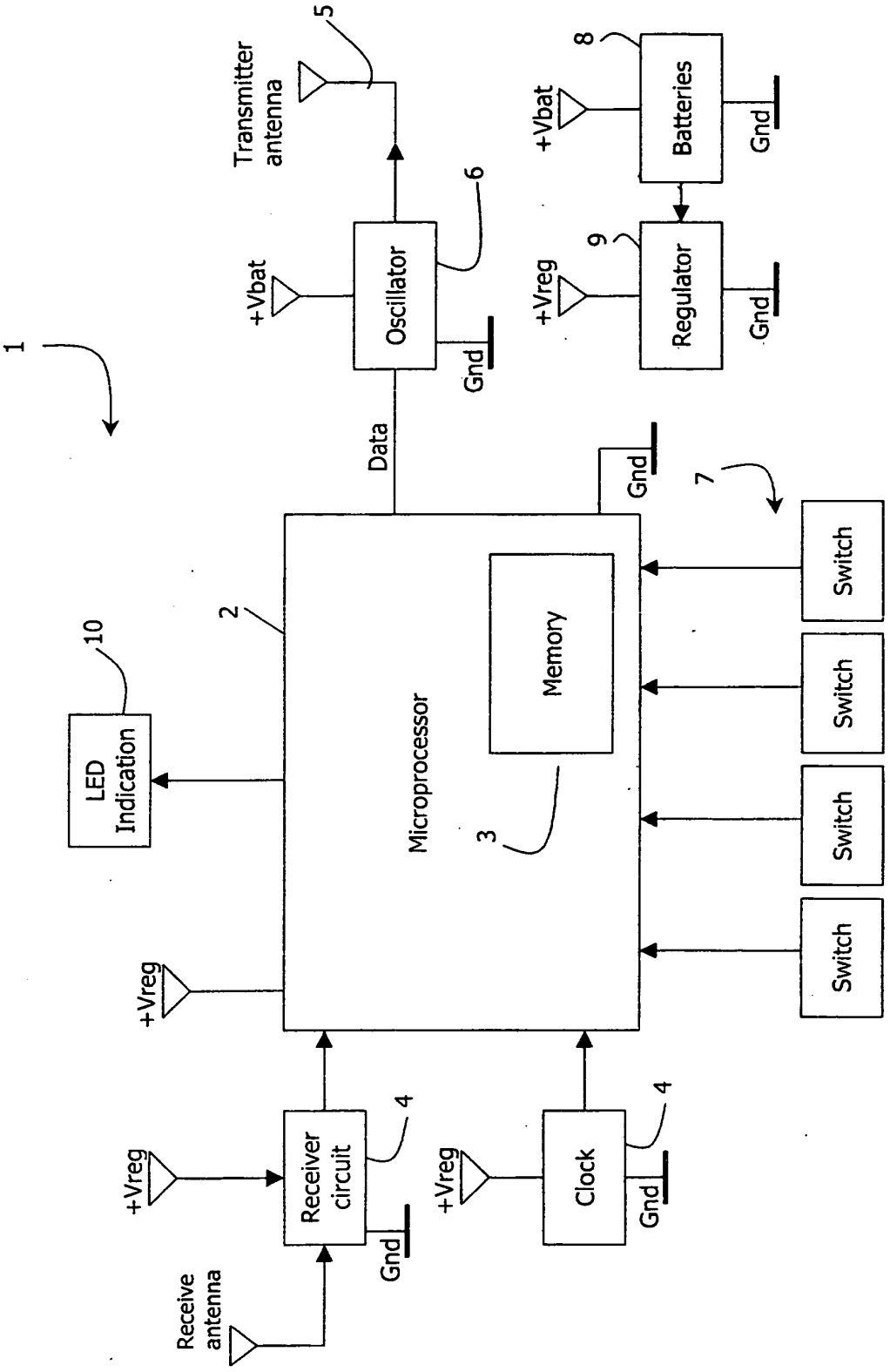
1
2
3
4
4
5
6
7
8
9
10
Microprocessor
Memory
Data
Gnd
Transmitter antenna
+Vbat
Oscillator
Gnd
+Vbat
Batteries
Gnd
+Vreg
Regulator
Gnd
LED Indication
+Vreg
+Vreg
Receiver circuit
Gnd
Receive antenna
+Vreg
Clock
Gnd
Switch
Switch
Switch
Switch

Fig. 1

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 0651119 B1 **[0002]**
- US 5661804 A **[0005]**