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

(11) EP 1 085 481 A2

(12) EUROPEAN PATENT APPLICATION

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

(51) Int Cl.[7]: **G08C 19/28**

(21) Application number: **00650129.0**

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

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

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

(71) Applicant: **PHISILOG RESEARCH LIMITED**
Foxrock, Dublin 18 (IE)

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

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

(54) A remote control transmitter

(57) A remote control group transmitter (1) stores an encryption key uniquely associated with the remote control group. The transmitter decrypts an encrypted group-specific site code in a teaching radiation signal. The site code is then used to generate the encryption key for operation of a shared group function. The transmitter, in use, encrypts the discrimination value and the hopping index with the encryption key. The serial number is transmitted, but is not encrypted A receiver of the group decrypts the encrypted code to determine the discrimination value and hopping index. The receiver validates a new transmitter by receiving and decrypting two encrypted codes in quick succession and checking that the serial numbers are the same and the second hopping index is valid with reference to the first hopping index.

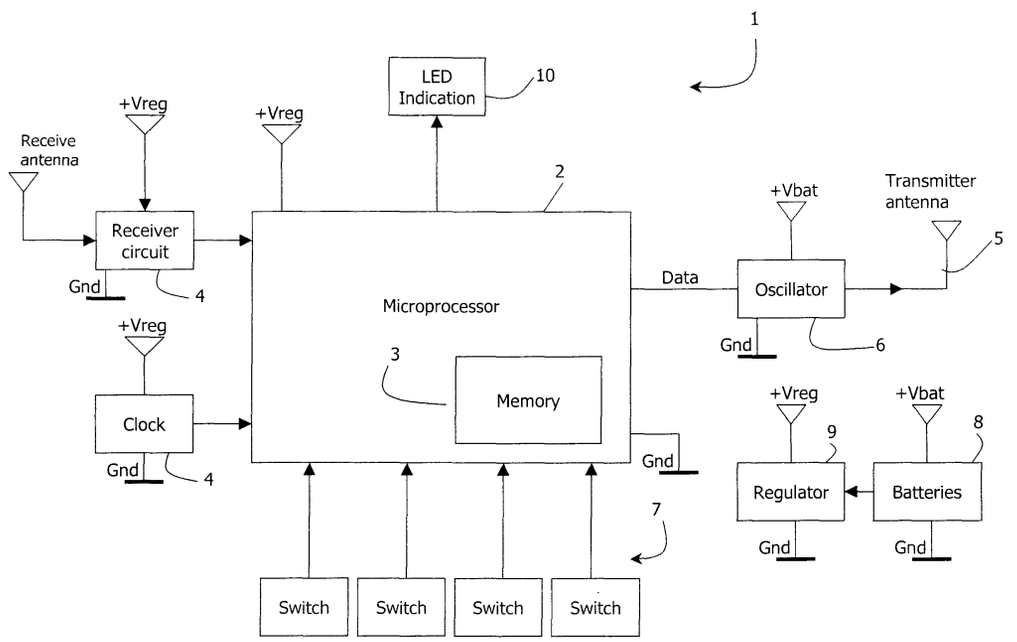

Fig. 1

EP 1 085 481 A2

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] According to the invention, there is provided a remote control group transmitter comprising a transmitting device, a user transmit button, a processor, and a memory, characterised in that,

the processor comprises means for:-

encrypting a valid code with an encryption key uniquely associated with the remote control group to generate an encrypted code, and

directing transmission of the encrypted code.

[0006] In one embodiment, the valid code is variable according to pre-set criteria.

[0007] In one embodiment, the valid code comprises a hopping index.

[0008] In another embodiment, the valid code comprises a combination of a fixed discrimination value known to the receiver and a hopping index.

[0009] In one embodiment, the transmitter comprises means for learning the encryption key in response to a teaching radiation signal.

[0010] In one embodiment, the 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 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 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 invention provides a remote control group master transmitter for teaching a transmitter as described above, the master transmitter comprising a memory, a processor, and a transmit device, wherein the 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] According to another aspect, the invention provides a receiver for a remote control group having a transmitter as described above, the receiver comprising a memory, an interface to a shared function, and a processor comprising means for controlling the shared function via said interface, wherein the processor further comprises:-

means for storing a decryption key uniquely associated with the remote control group,

means for decrypting a received encrypted code to generate a decrypted code, and

means for determining if the decrypted code is valid.

[0015] In one embodiment, the 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.

[0016] In another embodiment, the 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.

[0017] 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.

[0018] 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.

[0019] 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 described below.

[0020] 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.

[0021] 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.

[0022] 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 preset value.

[0023] 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.

[0024] 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.

[0025] The encryption key could alternatively be generated by only the master transmitter and taught to the receiver and the transmitters 1. However this suffers form the disadvantage of involving transmission of the encryption key.

[0026] 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

[0027] 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

[0028] 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.

[0029] 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.

[0030] 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.

[0031] The invention is not limited to the embodiments described but may be varied in construction and detail.

Claims

1. A remote control group transmitter comprising a transmitting device, a user transmit button, a processor, and a memory, characterised in that,
the processor comprises means for:-

encrypting a valid code with an encryption key uniquely associated with the remote control group to generate an encrypted code, and

directing transmission of the encrypted code.

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

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

4. A remote control group transmitter 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 transmitter as claimed in any preceding claim, wherein the transmitter comprises means for learning the encryption key in response to a teaching radiation signal.

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

7. A remote control transmitter as claimed in claim 6, wherein the 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.

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

9. A remote control group master transmitter for teaching a transmitter as claimed in any preceding claim, the master transmitter comprising a memory, a processor, and a transmit device, wherein the 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.

10. A receiver for a remote control group having a transmitter as claimed in any of claims 1 to 8, the receiver comprising a memory, an interface to a shared function, and a processor comprising means for controlling the shared function via said interface, wherein

the processor further comprises:-

means for storing a decryption key uniquely associated with the remote control group,

means for decrypting a received encrypted code to generate a decrypted code, and

means for determining if the decrypted code is valid.

11. A receiver as claimed in claim 10, wherein the 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.

12. A receiver as claimed in claim 11, wherein the 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.

13. A remote control group comprising a transmitter as claimed in any of claims 1 to 8 and a receiver as claimed in any of claims 10 to 12.

14. A remote control group as claimed in claim 13 further comprising a master transmitter as claimed in claim 9.

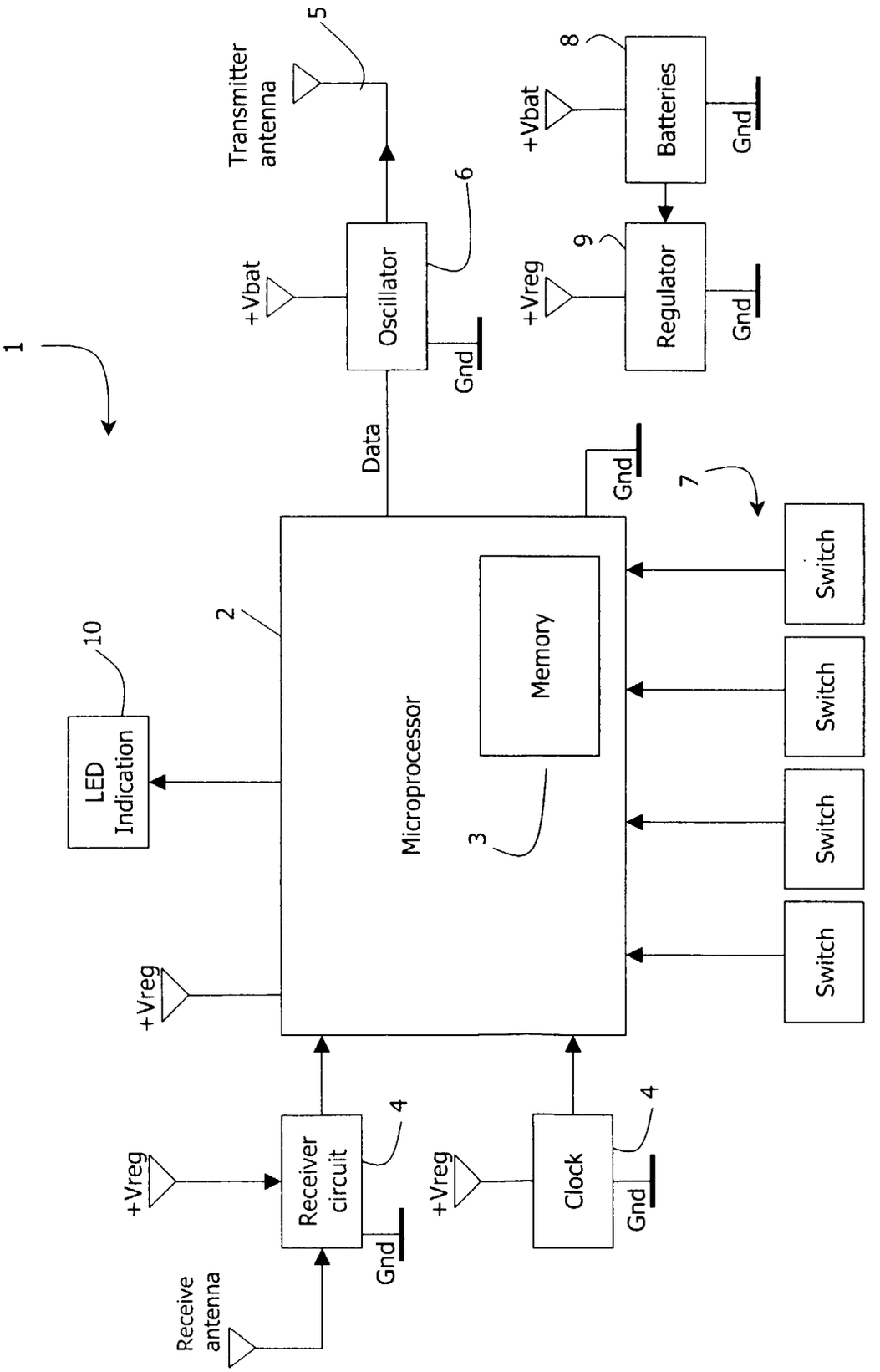
1
Transmitter antenna
5
+Vbat
Oscillator
6
Gnd
+Vbat
8
Batteries
Gnd
+Vreg
9
Regulator
Gnd
Data
Gnd
7
Switch
Switch
Switch
Switch
2
10
LED Indication
Microprocessor
Memory
3
+Vreg
+Vreg
Receiver circuit
4
Gnd
Receive antenna
+Vreg
Clock
4
Gnd

Fig. 1