(12) UK Patent Application (19) GB (11) 2576133 (13) A

(43) Date of A Publication 12.02.2020

(21) Application No: 1810614.6

(22) Date of Filing: 28.06.2018

(71) Applicant(s):
Mark Neath
28 New Road, WATER ORTON, Warwickshire, B46 1QU, United Kingdom

(72) Inventor(s):
Mark Neath

(74) Agent and/or Address for Service:
Vault IP Limited
5th Floor Cavendish House, 39 Waterloo Street, Birmingham, B2 5PP, United Kingdom

(51) INT CL:
G07C 9/00 (2020.01) ***B60R 25/24*** (2013.01)

(56) Documents Cited:
GB 2450154 A **EP 2575091 A1**
US 8841987 B1 **US 6429768 B1**
US 20170294062 A1 **US 20090061759 A1**

(58) Field of Search:
INT CL **B60R, G07C, H04K**
Other: **EPODOC, WPI**

(54) Title of the Invention: **Remote keyless system security device**
Abstract Title: **A signal jamming device for jamming remote keyless authorisation signals**

(57) The signal jamming device 30 has a transmitter 32 which transmits a jamming signal JS to jam a remote keyless authorisation signal KS. The jamming device preferably has a receiver to detect a keyless authorisation signal so the jamming signal can be transmitted in response, where the jamming signal preferably has a number of jamming signal frequencies. The jamming device preferably has a control to deactivate the jamming signal, which may be a button 34 or a switch. When the control is a switch the transmitter can be placed in persistent jamming mode or switched off. The jamming device may be used with a smart key 20 or may be integrated with a smart key.

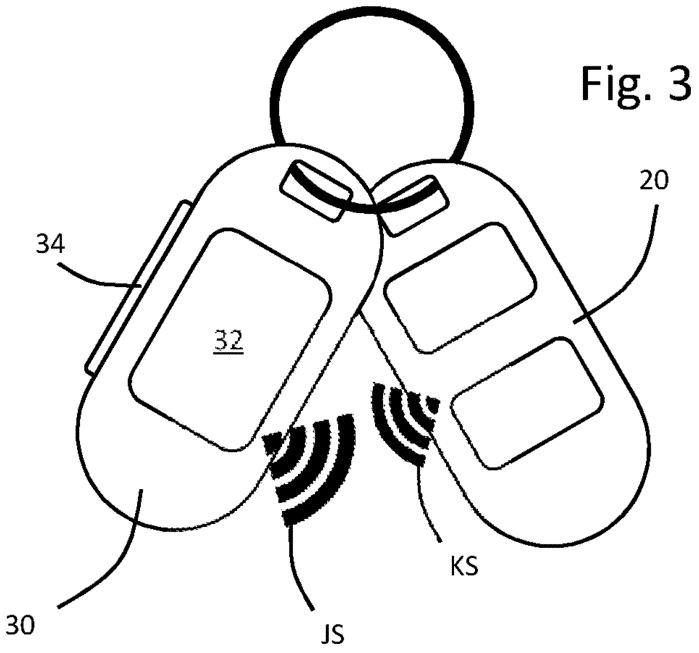

Fig. 3

GB 2576133 A

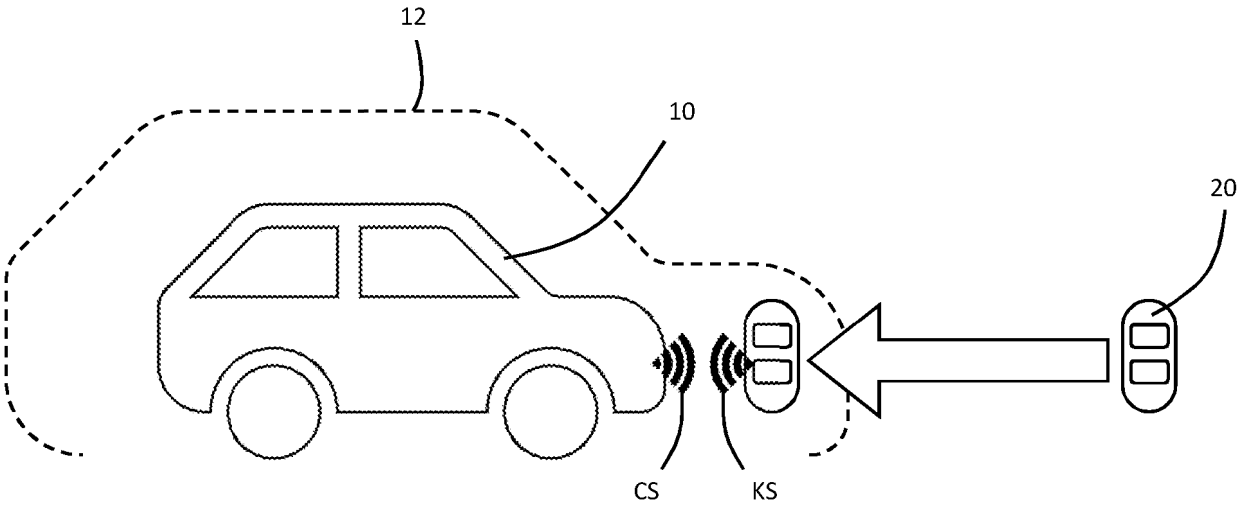

Fig. 1

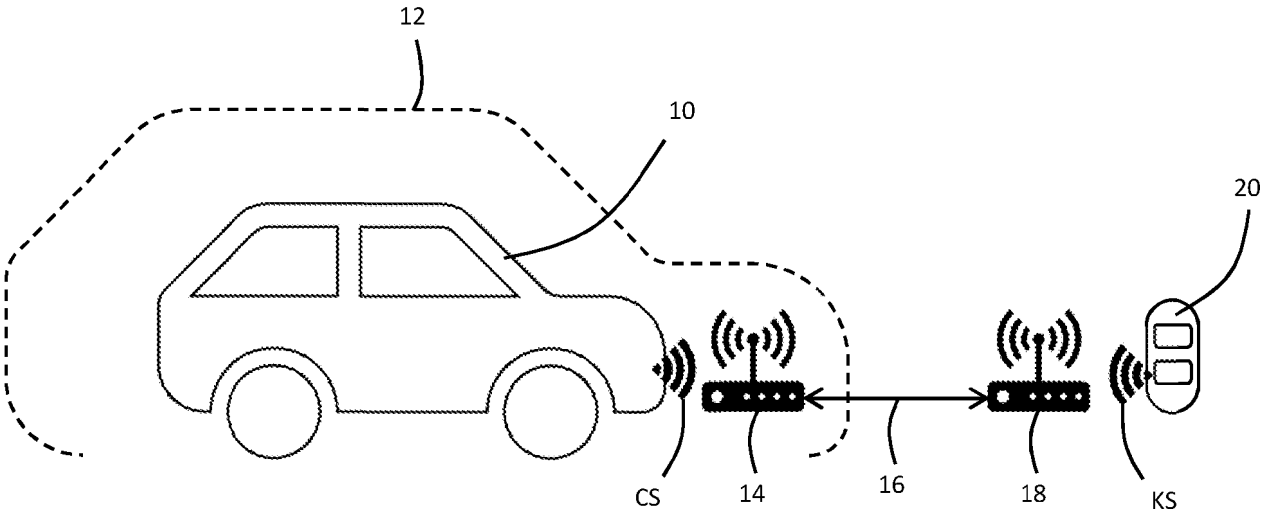

Fig. 2

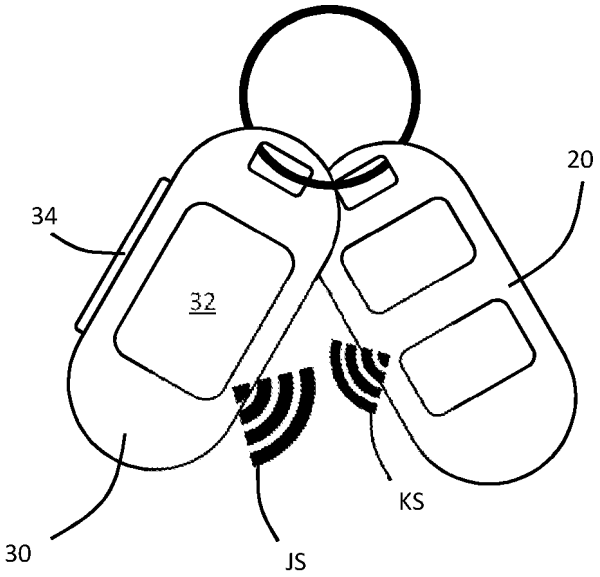

Fig. 3

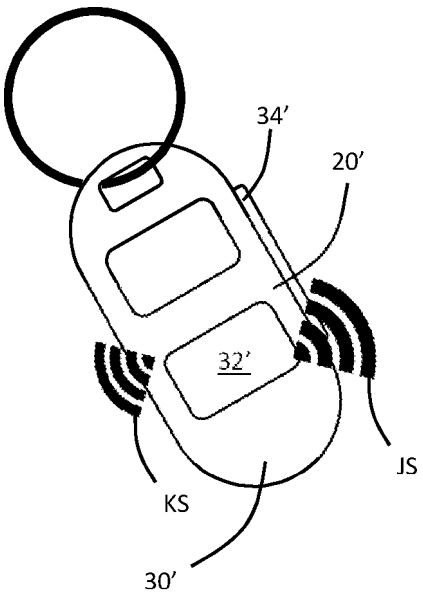

Fig. 4

Remote keyless system security device

The present invention is concerned with a remote keyless system security device. More specifically, the present invention is concerned with a device for preventing unauthorised keyless unlocking and ignition of vehicles fitted with automatic remote keyless entry (ARKE) and remote keyless ignition (RKI).

Many new vehicles feature some form of "remote keyless system". Generally, these systems can be differentiated as "remote keyless entry" (RKE) and "remote keyless ignition" (RKI). Many new cars feature both systems, as will be discussed below.

With "remote keyless entry" (RKE), the vehicle has an electronic lock which secures the doors in a closed condition, preventing entry. The electronic lock can be unlocked by the user manually pressing a button on a user unit (known as "manual remote keyless entry" (MRKE) or "remote central locking"). Many new cars employ a system in which the user unit is detected by proximity to the vehicle (known as "smart key" or "automatic remote keyless entry" (ARKE)). The latter system offers convenience to the user, as they merely need to have the user unit about their person, and do not need to search for it in coats, bags etc to unlock the vehicle. The present invention is concerned with ARKE.

With "remote keyless ignition" (RKI), instead of having an ignition switch requiring insertion of a key, the vehicle ignition may be started with a button. The button is only effective if the vehicle is able to detect the presence of the user unit. Again, this offers convenience to the user as they do not need to locate the key about their person to start the engine and drive the vehicle.

Both of these systems operate by establishing communication between the user unit and the vehicle by an electromagnetic signal. This is typically carried in the radio spectrum, more specifically in the UHF band, and even more specifically in the 300 – 400 MHz band. The signals are often encrypted to prevent duplication by unauthorised sources.

The user unit discussed above is typically still referred to as a "smart key" (whether or not is comprises a physical key) and as such the term "smart key" used hereinafter will refer to an electronic user unit whether or not it comprises a physical key.

Referring to Figure 1, there is shown a vehicle 10 fitted with ARKE and RKI. A smart key 20 is provided which, when moved within a detection zone 12 surrounding the vehicle 10 will cause the vehicle doors to be unlocked. The vehicle 10 transmits a signal VS, and the smart key KS.

There is a method of stealing cars fitted with the above remote keyless systems known as "scanning" or "relaying".

Referring to Figure 2, a large resonant pick-up coil (vehicle coil 14) is held adjacent to the car within the detection zone 12) which is connected by cable 16 to a similar coil (key coil 18) which is placed as close as possible to the position of the smart key 20. The signal broadcast by the vehicle 10 is picked up by the vehicle coil 14 and relayed to the key coil 18. The transponder in the smart key 20 is energised as if it was close to the car, car / key exchange takes place as normal and the response is "relayed" back to the car 10. The doors are therefore opened (ARKE) and the car will start (RKI).

The method is used to artificially close the physical gap between the car and the smart key. As many people keep their smart key close to the front door of the house it is often possible for the key coil to be positioned quite close to them. Such systems may also be used to close the gap between smart keys held in valet stands, or in a bag etc.

Various solutions have been proposed.

WO2004114227 discusses a device which provides a means of communication between the key or fob and car which includes a signal which is perceptible to humans. So, for example, sound or light can be used as a signal medium. In this way, the user will know if a relay attack is being carried out.

EP0908589 discusses the problem of relay attacks on keyless entry systems. The proposed solution allows the user to deactivate passive entry for a predetermined period of time. They system can also deactivate the passive mode after a predetermined time period, and also automatically disable passive mode for a predetermined period of time after locking the vehicle. A "porter" (better known as a "valet") mode is also disclosed in which certain areas of the car (e.g. the boot) are not accessible. As an additional measure against relay attack, the key is provided with an alert tone when it receives a signal from the car.

US7791457 discloses a system for identifying unauthorised access to a vehicle having a passive / keyless entry system. The device operates by having the car transmit two interrogation signals to the key- the second being at a high amplitude than the first. The key will only open the car when it detects this amplitude difference.

US20060044108 is concerned with passive keyless entry, and the threat of relay attack. The patent application discusses the detection of a relay attack by measuring transit time, given that the attack will "slow" the signal (compared to direct communication). It also acknowledges that transit time is not useful for high frequency relays. Instead, the system proposes that a deliberate delay time is built

into the system to provide an "additional, adjustable signal propagation delay" which can be detected and verified.

It is an aim of the present invention to provide an improved apparatus for overcoming the above-mentioned problem.

According to a first aspect of the invention there is provided a remote keyless security device comprising a transmitter configured to transmit a jamming signal to jam a remote keyless authorisation signal.

Advantageously, a relay attack would be defeated because the jamming signal would inhibit successful communication and authorisation between the vehicle and the smart key.

Preferably the jamming signal has a plurality of jamming signal frequencies. This allows the device to operate with a number of different vehicle types.

Preferably the device comprises a receiver configured to detect a remote keyless authorisation signal from a vehicle and / or a smart key, and to transmit the jamming signal in response to such detection. This avoids the need for the device to constantly transmit a jamming signal, which would be detrimental to battery life.

Preferably the device is configured for use as a key fob. Therefore it is preferably less than 10cm in maximum dimension, more preferably less than 5cm. Preferably it is suitable for attachment to a keyring.

The device may have a control for selective deactivation of the jamming signal. This allows the user to activate keyless entry.

Preferably the control is configured to deactivate the jamming signal for a predetermined period of time. Advantageously, the user will not leave the device in a state in which a relay attack is possible. The control may be a button.

The control may be a switch configured to place the transmitter into persistent "jamming on" and "jamming off" modes.

The invention also provides an assembly of a smart key and a remote keyless security device according to any preceding claim, in which the smart key is configured to transmit the remote keyless authorisation signal for providing remote keyless entry and / or ignition of a vehicle.

The invention also provides a smart key comprising an integrated remote keyless security device according to any of claims 1 to 12, in which the smart key is configured to transmit the remote keyless authorisation signal for providing remote keyless entry and / or ignition of a vehicle.

Embodiments of the present invention will now be described with reference to the accompanying drawings, in which:

FIGURE 1 is a schematic of a known car fitted with a remote keyless system;

FIGURE 2 is a schematic of the car of Figure 1 being accessed by a relaying attack;

FIGURE 3 is a schematic view of a first embodiment of the present invention; and,

FIGURE 4 is a schematic view of a second embodiment of the present invention.

Referring to Figure 3, there is shown the smart key 20, and attached thereto a jamming device 30 according to the present invention.

The jamming device 30 comprises a transponder 32 which is configured to detect communication between the vehicle 10 and smart key 20 and to transmit a jamming signal JS. The transponder 32 is powered by a battery. The jamming device 30 is configured to transmit the jamming signal JS upon detection of communication between the vehicle 10 and the smart key 20. The jamming signal JS is programmed to disrupt successful communication between the vehicle 10 and key 20 with a disruptive datastream.

The jamming signal JS is transmitted at a higher power (amplitude) than the key signal KS so as to ensure effective jamming.

The jamming device 30 comprises a control in the form of a button 34. The button 34 is connected to the transponder 32, and upon depression will deactivate the transponder for a predetermined period of time. In the present example, the transponder is prevented from transmitting the jamming signal JS for 10 seconds (although it will be understood that other times are possible).

In this embodiment, the jamming signal is provided at all known frequencies for keyless entry systems. In this way, the device will work with all known systems without reprogramming.

Turning to Figure 4, a smart key 30' has the transponder 32' and button 34' integrated therewith. The key can therefore transmit the jamming signal JS at the same time as the key signal KS to disrupt the latter.

Variations fall within the scope of the present invention.

The control may be in the form of an on / off switch instead of a button 34. In this way, the user can choose to leave the device 30 in a persistent state of “jamming on” or “jamming off”.

The jamming signal JS may only be transmitted at the frequency of the key signal KS.

Claims

1. A remote keyless security device comprising a transmitter configured to transmit a jamming signal to jam a remote keyless authorisation signal.

2. A remote keyless security device according to claim 1, in which the jamming signal has a plurality of jamming signal frequencies.

3. A remote keyless security device according to any preceding claim, comprising a receiver configured to detect a remote keyless authorisation signal from a vehicle and / or a smart key, and to transmit the jamming signal in response to such detection.

4. A remote keyless security device according to any preceding claim, being less than 10cm in maximum dimension.

5. A remote keyless security device according to any preceding claim, being suitable for attachment to a keyring.

6. A remote keyless security device according to any preceding claim, comprising a control for selective deactivation of the jamming signal.

7. A remote keyless security device according to claim 6, in which the control is configured to deactivate the jamming signal for a predetermined period of time.

8. A remote keyless security device according to claim 7, in which the control is a button.

9. A remote keyless security device according to claim 6, in which the control is a switch configured to place the transmitter into persistent "jamming on" and "jamming off" modes.

10. An assembly of a smart key and a remote keyless security device according to any preceding claim, in which the smart key is configured to transmit the remote keyless authorisation signal for providing remote keyless entry and / or ignition of a vehicle.

11. A smart key comprising an integrated remote keyless security device according to any of claims 1 to 10, in which the smart key is configured to transmit the remote keyless authorisation signal for providing remote keyless entry and / or ignition of a vehicle.

Intellectual Property Office

Application No:	GB1810614.6	**Examiner:**	Mr Robert Alexander
Claims searched:	1-11	**Date of search:**	17 December 2018

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
X	1-11	US 8841987 B1 (STANFIELD) see column 5 line 16 to column 8 line 36 and the figures.
X	1-11	US 2017/0294062 A1 (VAN WIEMEERSCH) see paragraphs 3, 11, 15, 18, and 19 in particular and figure 1.
X	1-11	US 2009/0061759 A1 (STODDARD) see paragraphs 2, 14, 25, 35, 49-67 and figures 1 and 3.
X	1-4, 6-10	US 6429768 B1 (FLICK) see column 2 lines 22-52 and column 3 line 53 to column 6 line 42.
X	1-4, 6-10	EP 2575091 A1 (DELPHI TECHNOLOGIES) see paragraph 29 and figure 1.
X	1, 2, 6-10	GB 2450154 A (JEREMY ROBIN AND STANLEY RONALD) see page 2 lines 29-32 and page 5 lines 20-32 and figure 1.

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

Worldwide search of patent documents classified in the following areas of the IPC

B60R; G07C; H04K

The following online and other databases have been used in the preparation of this search report

EPODOC, WPI

Intellectual Property Office

International Classification:

Subclass	Subgroup	Valid From
G07C	0009/00	01/01/2006
B60R	0025/24	01/01/2013