(12) UK Patent Application (19) GB (11) 2 288 262 (13) A

(43) Date of A Publication 11.10.1995

(21) Application No 9506279.0

(22) Date of Filing 28.03.1995

(30) Priority Data
(31) 4411449 (32) 01.04.1994 (33) DE

(71) Applicant(s)
Mercedes-Benz AG

(Incorporated in the Federal Republic of Germany)

136 Mercedesstrasse, D70327 Stuttgart,
Federal Republic of Germany

(72) Inventor(s)
Horst Brinkmeyer
Michael Daiss
Gunter Schwegler
Bertolt Kruger

(74) Agent and/or Address for Service
Jensen & Son
70 Paul Street, LONDON, EC2A 4NA, United Kingdom

(51) INT CL^{6}
B60R 25/04 , E05B 49/00

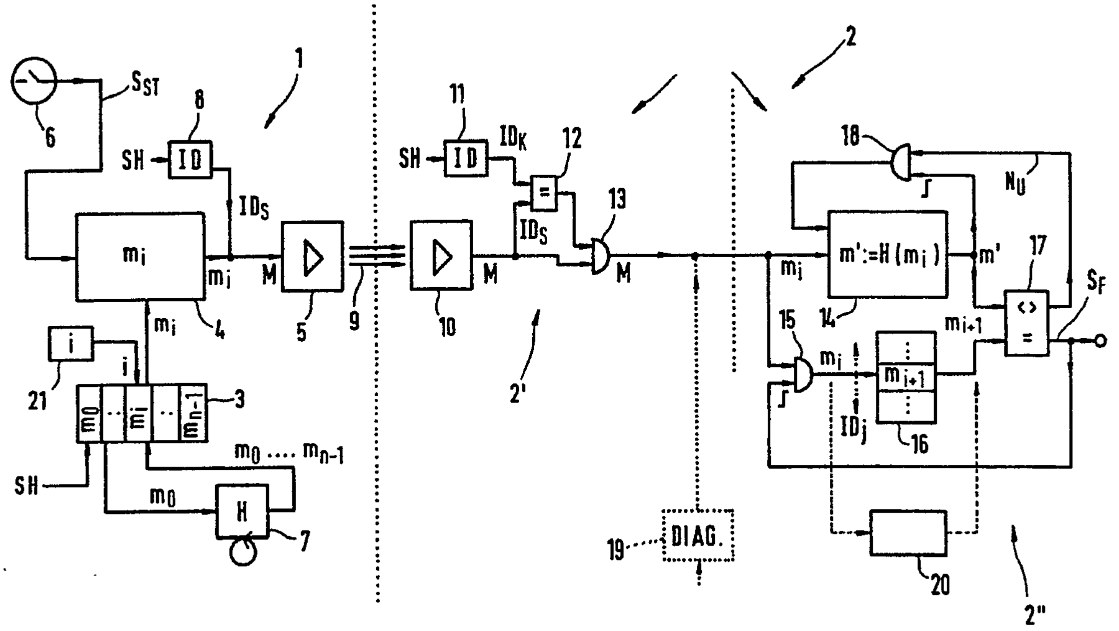
(52) UK CL (Edition N)
G4H HTG H1A H13D H14A H14B H14D
U1S S1820

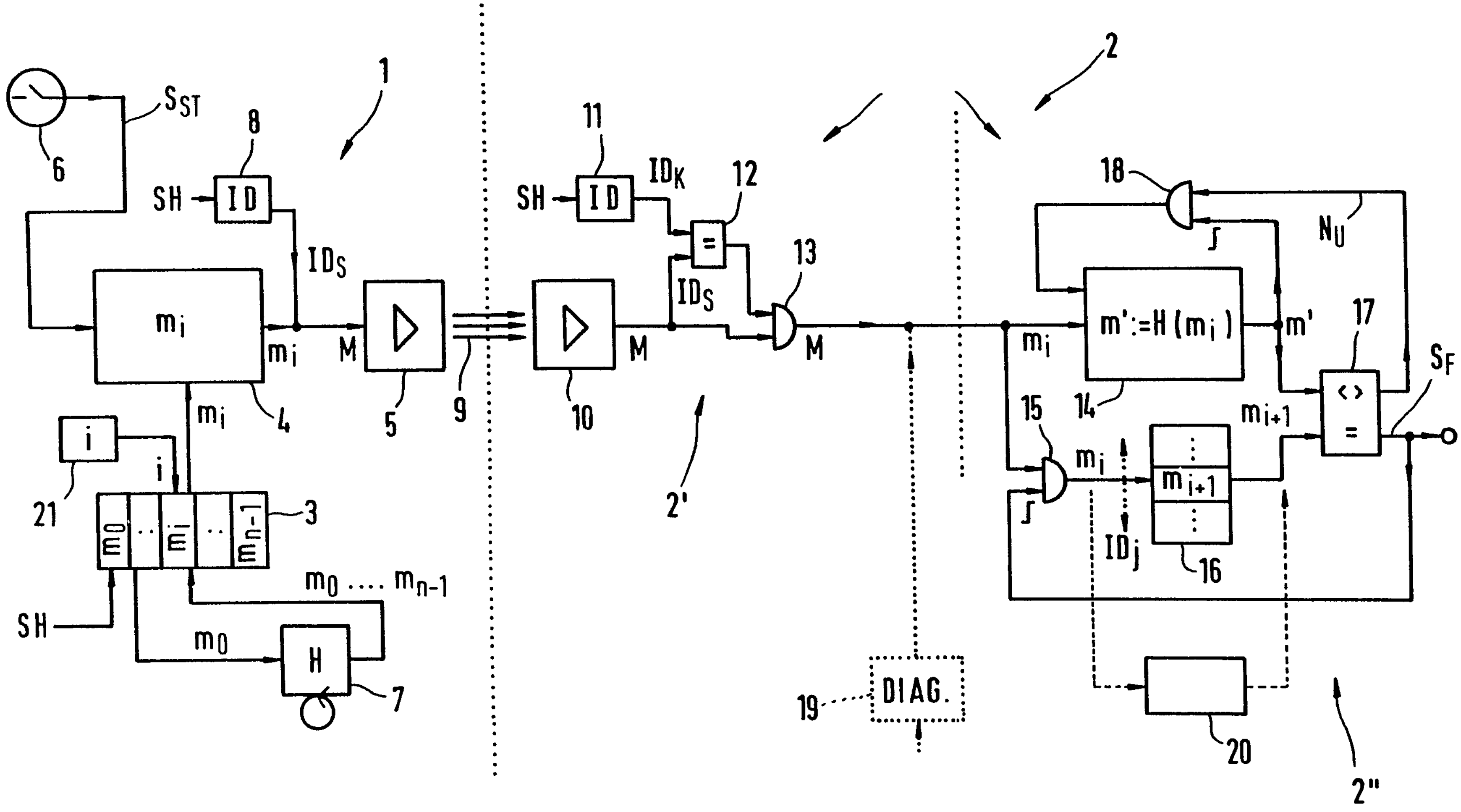
(56) Documents Cited
GB 2282687 A

(58) Field of Search
UK CL (Edition N) G4H HTG
INT CL^{6} B60R , E05B
Online:WPI

(54) **Vehicle security device with electronic use-authorization coding**

(57) The vehicle security device involves an encryption method which operates on the basis of a one-way function and in which it is only absolutely necessary to store secret code information at the key end 1, specifically in the form of different inverse values of a one-way function while it is only necessary for the one-way function values corresponding to these inverse values to be present at the vehicle end 2, the reading out of which inverse values does not permit unauthorized manufacture of a false key because of the virtual non-reversibility of the one-way function.




1
2
2'
2"
6
S_{ST}
8
SH
ID
ID_S
m_i
M
4
5
9
3
21
i
m_0
m_i
m_{n-1}
SH
m_0
$m_0 \ldots . m_{n-1}$
H
7
11
SH
ID
ID_K
12
=
ID_S
13
M
10
M
19
DIAG.
18
N_U
$m':=H(m_i)$
m'
17
<>
=
S_F
14
15
m_i
m_{i+1}
ID_j
16
20

2288262

Vehicle security device with electronic use-authorization coding

The invention relates to a vehicle security device with electronic use authorization coding having a user-end key unit for successfully transmitting items of user code information which differ from one another, a vehicle-end piece of equipment for receiving the user code information which is transmitted respectively by a key unit, for determining an item of actual authorization information which is dependent on the received user code information and comparing it with an item of desired authorization information which is present at the vehicle end and for generating, in a comparison-dependent way, an item of use-enabling information.

Such vehicle security devices are known, for example as electronic disabling facilities which operate according to a so-called alternating code method for protecting the vehicle against unauthorized use by a third party, cf. for example the company brochure "Diebstahlschutz für das Auto [Protecting cars against theft]" from TEMIC TELEFUNKEN microelektronik GmbH dated August 1993. In comparison with fixed code methods which were customary in the past, as described for example in the German Offenlegungsschrift DE 29 11 828 A1, in such alternating code methods safeguarding against unauthorized use of the vehicle after one or more of the code transmission protocols have been intercepted is enhanced by the code information changing at each so-called authentification process, i.e. at each testing process of the use authorization. This code change can only be realized from the key end to the vehicle end in compliance with the omnidirectional code information transmission known from the fixed code method by a secret item of base counting information and an algorithm being stored both at the key end and at the vehicle end, according to which algorithm the successive items of code information can be derived from the base number so that at the vehicle end the user authorization can be tested by respectively comparing the code information produced at the vehicle end with the code information transmitted at the key end. A difficulty is posed in these unidirectional systems by the synchronization of the key end and vehicle end, which on the one hand is desirable, for example after a defect has been eliminated or when a replacement unit is being used at the key end or vehicle end, but on the other hand is particularly critical for security since an unauthorized person may, in future, possible gain unrestricted authorization as an authorized user by means of a successful synchronization manipulation. Alternatively, it is known to provide, after each successful authentication by means of compulsory synchronization from the key end and vehicle end each with a new, randomly selected or deterministically specified authorizing item of code information for the next authentication, cf. for example the German Offenlegungsschrift DE 32 34 539 A1 and the patent document DE 33 13 098 C1. However, such controlled synchronization requires a bidirectional exchange of data which is facilitated in a wireless fashion or via electrically conductive contact between the key unit and a piece of vehicle equipment which is involved in the process.

Moreover, in addition to the alternating code methods which operate during an authentication with unidirectional data transmission, so-called symmetrical encryption methods are known in which the authentication takes place by means of bidirectional data exchange, one secret coding algorithm of the same type being stored on the one hand at the key end and at the other end at the vehicle end respectively. This algorithm generates a respective item of code information in response to an item of input information, e.g. an item of random counting information, fed to both ends, the key-end code information being subsequently transmitted to the vehicle end and tested there for correspondence with the code information generated at the vehicle end. A method of this kind is described in the

German Offenlegungsschrift DE 32 25 754 A1.

Consequently, all the abovementioned methods require the storage of an item of secret information at the vehicle end. Thus, there is not only a certain risk of unauthorized reading out of an item of secret information from the vehicle end but additionally care must be taken that such secret data information should be provided at the vehicle end in a protected way, which makes corresponding logistic outlay at the vehicle manufacturer's and in garages necessary in which this secret vehicle-specific information is to be fed into piece of replacement equipment.

The invention is based on the technical problem of providing a vehicle security device which provides a relatively high degree of protection against unauthorized use of a vehicle by third parties together with a relatively low degree of outlay, in particular even by means of unidirectional data transmission, and convenient control, in which case it is in particular impossible for a non-authorized person, simply by intercepting an authentication process or reading out an item of vehicle-end code information, subsequently to use the vehicle without authorization by means of successful authentication using the intercepted or read-out information, and in which case it is not necessary to store secret items of information at the vehicle end.

According to the present invention there is provided a vehicle security device with electronic use-authorization coding, having

- a user-end key unit for successfully transmitting items of user code information which differ from one another,
- a vehicle-end piece of equipment for receiving the user code information which is transmitted respectively by a key unit, for determining an item of actual authorization information which is dependent on the received user code information and comparing it with an item of desired authorization information which is present at the vehicle end and for generating, in a

comparison-dependent way, an item of use-enabling information, wherein: the successively transmitted user code information contains an inverse value for a one-way function,

- the desired authorization information is in each case the one-way function value of the inverse value contained in an item of associated user code information and
- the determination of the actual authorization information from the received user code information includes the formation of the one-way function value of the inverse value contained in the received user code information.

The vehicle security device offers a relatively high degree of protection against unauthorized use of the vehicle by third parties with a comparatively low outlay. In particular, a vehicle-end storage of an item of secret information is not absolutely necessary, which saves on security logistics and the vehicle manufacturer's and garages's costs. This further avoids associated security risks and additionally has the result that false keys with which successful authentication would be possible cannot be manufactured by reading out the code information contained at the vehicle end. The omission of logistical security measures is then a particularly important factor if a plurality of pieces of equipment is involved in authentication at the vehicle end so that it is made uneconomical to bypass the disabling facility by simply replacing one or a small number of pieces of equipment involved in authentication. The code security of the authentication is based on the property, in accordance with its definition, of a mathematical one-way function, that namely the algorithm for calculating a one-way function value to form an inverse value is comparatively simple, but on the other hand the acquisition of an inverse value which is associated with a given value of a one-way function is not possible within an available time period with a practically realizable computational outlay. Therefore, the property of a function of being a one-way function also depends on the computer capacity available at the current state of computer technology, such one-way functions, e.g. in the form of so-called hash functions, are known and are principally used for protecting messages in cryptography, it being possible nowadays for a number of approximately 2^{50} calculation and memory processors of hash values to be assumed as the upper limit for the computational outlay which can be practically coped with. Because of the virtual non-reversibility of the one-way function, the one-way function values at the vehicle end do not have to be treated as secret values since even unauthorized reading out of the said values from the vehicle would not permit an unauthorized person to discover the associated inverse values and thus produce an electronic copy of the key. The security of the system is also given by the fact that a new item of inverse value code information is transmitted for each authentication attempt. Depending on the result of the comparison of actual and desired authorization information, the authentication unit at the vehicle end outputs an item of use-enabling information which in the case of a positive authentication attempt leads to an associated electronic disabling facility being deactivated and in the case of a negative authentication attempt causes it to remain activated, the electronic disabling facility ensuring that after the ignition key is withdrawn at least one piece of equipment which is at the vehicle end and is relevant for access to the vehicle or for the operation of the vehicle, for example a locking control, an engine control device etc., is kept in a disabling position.

One embodiment of the invention realizes in an advantageous, simple manner the provision of the inverse values stored at the key end in that this sequence of values is formed by successively executing the one-way function, after which the said sequence is read out backwards during operation of the key, i.e. from the last inverse value to be determined to the initial one. At the vehicle end this provides the technical advantage in terms of memory that not all the one-way function values associated with the inverse values have to be stored. Instead, the initial storage of the one-way function value which is associated with the first inverse image to be transmitted is sufficient for the provision of the desired authentication information, after which whenever there is a successful authentication using the same key unit this storage information is overwritten with the inverse value information transmitted for this authentication since a previously transmitted inverse value is always in fact the one-way function value of the inverse value transmitted subsequently.

With a further embodiment of the invention, memory space can be saved at the key end in that not all the inverse values required over the service life of the key unit are kept stored but rather samples at selected intervals of the entire sequence of image values and a respectively current value range between two samples. Whenever a current range has been used up as far as a prescribable remainder, the one-way algorithm stored at the key end can be used to generate a new current range starting from the next sample by recursive application of the one-way function, and to store it.

By means of one embodiment of the invention, a so-called capture range is formed at the vehicle end which capture range makes it possible, to a prescribable degree, to synchronize the vehicle end with the key end again if the synchronization has been lost as a result of one or more transmission activities at the key end for which there was no corresponding reception activity at the vehicle end. If the one-way function value of a received inverse image as actual authentication information does not correspond to the instantaneous vehicle-end desired authentication information, the capture range permits a recursive one-way function information to be run through for a prescribed maximum number of repetitions, the one-way function value which is produced in each case from the previous actual authentication information serving as new actual authentication information. If correspondence with the desired authentication information stored at the vehicle end is detected with actual authentication information which has been newly determined in this way, this is evaluated as a positive authentication attempt and the disabling facility is then correspondingly deactivated and the transmitted inverse value information is stored as new desired authentication information for the next authentication attempt with this key. If the capture range is selected to be as large as the power of the total inverse value sequence possible in the key unit, this additionally permits unauthorizing replacement key to be adopted into the system in an advantageously simple way while simultaneously the replaced key automatically becomes invalid. For this purpose, the replacement key is preferably initialized by means of a development according to Claim 5, for which all that is necessary is the storage by a key CPU of a single secret starting value for the formation of one-way function values for the initiation of the first key and of all further keys which replace the previous key successively as required.

The one-way function used can be, one of the hash functions known from cryptography, specifically the RIPEMD algorithm, which, according to the current state of cryptography, can be assumed to have the required one-way function properties.

In a further embodiment of the invention, a plurality of pieces of equipment at the vehicle end are involved in parallel in the authentication, for which purpose they can be favourably connected via a common data bus. This decentralized distribution of authentication which can extend over all the vehicle-relevant pieces of equipment, makes bypassing the disabling device by mechanical intervention consisting in replacing equipment substantially more difficult since all the pieces of equipment affected by the authentication and the disabling facility would then have to be replaced in order to make it possible for the vehicle to be used by an authorized person who does not have the means of achieving successful authentication. The pieces of equipment involved, in particular control devices for the electronic systems of the vehicle, can be selected here to be such that replacing them would require an unreasonably high outlay in relation to the benefit gained, and would therefore be unattractive.

In another embodiment of the invention, the locking control of the vehicle is included in each case in the authentication so that it is not only that the vehicle cannot be started without authorized authentication, it cannot be opened either without violence. If further pieces of equipment are involved, these may be connected to one another for example by means of a data bus, and to the locking control, a single vehicle-end receiver for the data transmitter at the key end then being sufficient, it being possible for the said receiver to be assigned for example to the locking control.

One embodiment of the invention according to Claim 9 has the advantage that, by means of the initial identification testing with respect to the vehicle and the key, it is firstly detected whether legitimized hardware units are connected to one another before the actual authentication process is carried out. The unnecessary activation of authentication operations, which cannot succeed because of an incorrect key/vehicle combination, are avoided in this way.

One embodiment of the invention according to Claim 10 permits the use of a set of keys with a plurality of keys for the vehicle in a manner which is advantageous for circuit technology and maintains the one-way function coding algorithm.

A preferred embodiment of the invention is illustrated in the drawing and described below, by way of example.;

The single figure shows a block diagram of a vehicle security device with electronic use-authorization testing by means of unidirectional transmission of code data.

The vehicle security device contains at the user end a plurality of, e.g. eight, electronic keys 1, one of which is shown by way of example, and at the vehicle end a plurality of pieces of equipment 2 which are involved in the protection of use, one of which is a locking control whose design is illustrated to serve as an example for the other pieces of equipment in the figure while the other pieces of equipment are the other control devices of the vehicle's electrical system. Here, the circuit component 2′ which is illustrated in the figure at the vehicle end to the left of the right-hand, dotted dividing line while the circuit component 2" which is located to the right of this dividing line is present in an identical form for all the pieces of equipment involved. All the pieces of equipment 2 involved in protection communicate with one another and with the receiver-end circuit component 2′ present in the locking control via a CAN bus or alternatively via another data exchange link in the vehicle. The key units and pieces of equipment 1, 2 are each equipped here with a processor chip in which the function units which are each illustrated in block form in the figure and described below are largely implemented by means of software.

The key units 1 each have a transmitter 5 with which key-end data can be transmitted in coded form via an infrared link 9 to the vehicle end where they can be received and subsequently decoded by a receiver 10 in the input circuit component 2′ of the locking control 2. Furthermore, each key unit 1 has a unit 7 for recursively generating one-way function values of a Hash function H which is used for example in cryptography, the RIPEMD function which is known from "Ripe Integrity Primitives, Final report of RACE Integrity Primitives Evaluation [R1040] [June 1992], Part III Recommended Integrity Primitives, Chapter 3 RIPEMD, pp67-109" being used here specifically as hash one-way function. A one-way function is defined here as a mathematical function for which the function value of a given inverse value can be determined unambiguously and comparatively easily from its domain while it is not possible, even with the maximum practically available computational power available to find an inverse value for a given one-way function value. The bit length of a RIPEMD function value is 16 bytes, it being sufficient for the present purpose of providing vehicle security to transform the 16 byte value into a shortened 8 byte value by means of a suitable algorithm in order to save memory space. With this hash function value generating unit 7, a number n of values are produced by repeated application of the hash function starting with a starting value m_0 and stored as inverse value in an inverse value memory 3 which can be read out backwards, i.e. starting with the last value m_{n-1} of the inverse value sequence $[m_0, \ldots, m_{n-1}]$ successively into a coding stage 4 by means of a display counter 21. The number n determines the maximum number of authentication attempts which can be triggered by the key unit 1 during its service life and is to be selected appropriately, for example n=100,000 for approximately 20 activations per key per day with a service life of the key of approximately 10 years. The reading out of the buffer 4 can be controlled by means of a starting signal S_{ST} which is generated by means of a user key 6.

In order to store hardware identification data which comprise a vehicle-specific and a key-specific item of information, each key unit 1 has an identification data memory H whose data is connected by the key unit 1 to the coded inverse value information 11 originating respectively from the coding stage 4 to form the user code information M to be transmitted as a message. In order to initiate an authentication, a user key 6 is provided whose starting signal S_{ST} can be transmitted to the vehicle-locking control 2.

At the vehicle end the information input-end circuit component 2′ of the locking control 2 contains an identification data memory 11, an identification data comparator 12 and a gate function 13. The comparator 12 compares the identification data information ID_S extracted in this locking control device circuit component 2′ from the received user code information M with the identification data information ID_K stored in the vehicle-end identification data memory 11 and supplies its output signal to a control input of the gate 13 whose other input is supplied with the user code information signal 11. Optionally, a diagnostic interface 19 can be connected to the locking control 2, as indicated in the figure by dotted lines.

The locking control circuit component 2" which is shown in the figure to the right of the right-hand dotted dividing line and is also present in identical form in all the other pieces of equipment 2 involved in the vehicle security system contains, again realized by means of software, a unit 14 for calculating hash function values and a gate function 15, to both of which the inverse value information m_i contained in the user code information M can be fed. The output of this gate 15 is connected to a desired authorization information memory 16 with a number of memory locations corresponding to the number of key units 1, the individual memory locations being capable of responding independently of the detected key identity ID_j, i.e. the key number. The output of this memory 16 is in turn connected to an input of a comparator block 17 to which the output signal m′ of the hash function value generating unit 14 can be fed via a further input. This output signal m′ is also fed to a further gate block 18 whose control input is supplied with a non-correspondence signal N_U of the comparator 17. In contrast, when correspondence is detected the comparator 17 generates a use-enabling signal S_F to cancel a state which blocks the operational capability of the software of the respective piece of equipment 2 and is part of an electronic disabling facility which keeps all these pieces of equipment disabled. The use enabling signal S_F, which represents successful authentication, i.e. use authorization testing, does not leave the associated piece of equipment and preferably not even the chip area which provides a high degree of security against unauthorized external feeding in of the use-enabling information and is also fed as a control signal to the gate block 15, which is supplied with the transmitted inverse value information m_i, in order to permit this information to be stored as new set authorization information. In order to carry out special functions via the diagnostic interface 19, possibly connected to the locking control, or a key unit 1 an additional desired authorization memory 20 for special functions may be provided parallel to the normal desired authorization information memory 16, as indicated by broken lines in the figure.

As mentioned above, all the pieces of equipment 2 involved in the authentication process are simultaneously also involved in an electronic disabling facility which is set by switching off the ignition and can be deactivated again by a subsequent successful authentication process. Since the same authentication operations are carried out in all these pieces of equipment 2, all these units 2 become operational again simultaneously in the event of an authorized request for use while in the event of an unauthorized request for use at least one remains disabled. The distribution of the authentication process to all these pieces of vehicle equipment and the corresponding disabling of the same has the advantage that the vehicle cannot continue to be used by simply replacing one or a small number of pieces of equipment by bypassing the necessity for authentication. Instead, all these pieces of equipment would have to be replaced, which would be so expensive that such an attempt at unauthorized use by third party would be unattractive.

Details are given below on the mode of operation of the vehicle security device constructed as described.

The entire sequence begins initially before the vehicle is started up with the necessary initialization processes at the key manufacturer or a central key processing facility SH designed for this purpose. Here, a secret random value R_0 is initially produced for each key on an individual basis. The secret inverse starting value M_0 is then calculated from this random value R_0 by multiple, e.g. 400,000 times, successive application of the hash function and fed into the inverse value memory 3 in the respective key unit 1. The hash function values which are initially not used between the secret initial random value R_0 and the inverse starting value m_0 can serve as resources for a key replacement, described further below, for which purpose the associated initial random value R_0 is stored in a protected memory of the central key processing facility SH. In addition to the inverse starting value m_0, during the production of the key unit 1 the identification data ID_S are also fed into the associated memory 8, these data also containing, in addition to vehicle-specific data, a key number which distinguishes from one another the key units which are simultaneously valid for one vehicle. With the exception of the key number, the identification data of the key unit 1 which are simultaneously valid for one vehicle are identical and consequently form a kind of key set number. In parallel with this, the identical identification data are made available by the central key processing facility SH to be fed into the associated memory 11 of the locking control. In addition, in the central key processing facility SH during the initialization, starting from the inverse starting value m_0 the next n recursive hash function values $[H^J[m_0]; J=1, \ldots n-1]$ were all calculated in advance and the final value m_n obtained is passed on, as key-specific starting value for the desired authorization information for the vehicle-end initialization of the associated memory location of the respective desired authorization information memories 16, together with the identification data to the manufacturer of the vehicle.

Using the initialization data received from the central key processing facility SH the vehicle-end initialization is also carried out by the manufacturer of the vehicle by feeding a vehicle-specific hash function value, which is part of a hash function value sequence also generated in the central key processing facility SH, into the special hash function value memory 20, specifically depending on the security requirement to terminate production at the vehicle manufacturer or during the installation of the equipment on the production line or in a garage. In order to initialize the desired authorization information memory 16, in the course of production each memory location, assigned to a specific key unit 1, of these memories 16 of all the involved pieces of equipment 2 are loaded with the starting value m_n which is made available for this on a key-specific basis by the central key processing facility HS. For this purpose, the operator must obtain authorization via the diagnostic interface 19 and the hash function value which is stored in the special function memory 20 on a vehicle-specific basis, before said operator can form the first initialization by overwriting the initial value 0 with the key-specific initial value m_n of the desired authorization information, the memory location of the desired authorization information memories 16 being protected against normal overwriting as long as they contain the value zero. The special function memory 20 serves here as a transport protection for the pieces of equipment but, depending on requirements, may permit further special functions to be carried out. During this equipment initialization it must be ensured that the zero values of all the memory location for the different keys of one set are overwritten in order to prevent later unauthorized initialization by third parties. Alternatively, it is possible to pass on the starting value m_n of desired authorization information to the vehicle end for initialization when a first key actuation occurs. If a piece of equipment 2 which is involved in the process is replaced during repairs there may additionally be provision to initialize the newly inserted unit with the starting values which are automatically present in the other units by means of the CAN bus, which automatically ensures that all the starting values are overwritten to zero. In order to distinguish whether the information M which is fed to a piece of equipment 2 contains a normal authentication or a special function operation, the fed-in information M has, in addition to the identification data at which comprise approximately 8 bytes and the inverse image information which is shortened to 8 bytes, additionally a function code for which one data length of 1 byte is sufficient.

After initialization has taken place, each key unit 1 generates with the first connection to the power supply the other n-1 value, via its hash function value generating unit 7 from the stored starting value m_0 by repeated n-1-times, application of the hash function to the respective function value previously obtained and stores the obtained value sequence as an inverse value sequence in the appropriate memory 3 for successive reading out backwards, the associated counter 21 being initially set to the value n-1 and being reduced by one each time the activation key 6 is actuated. Since the storage of these for example 100,000 16-byte values requires appropriate space, the following, memory space-saving alternative process is possible. Selected values of the generated hash function value sequence $[m_0$ to $m_{n-1}]$, for example only a hundredth value, is permanently stored in the memory 3 as samples. Additionally, in each case an instantaneously present section of the value sequence $[m_0$ to $m_{n-1}]$ between two samples which consists e.g. of 100 values in each case is stored in the memory 3 so that in this way at any time only 1100 8-byte values have to be stored in the memory 3. As soon as the end of an instantaneous value sequence section is reached as a result of ongoing use of the key, the formation 7 of hash function value is activated with the next sample as input information in order to generate the next value sequence section between two samples, after which the used-up value sequence section is overwritten with the newly calculated one. Here, from the point of view of low memory requirement, the uniform memory distribution for the samples and for the region between two samples is even better, each memory component then containing the number of memory locations which corresponds approximately to the root of the power n of the entire value sequence [m_0 to m_{n-1}]. In order to make the memory requirement as low as possible it is alternatively possible only to keep the initial value m_0 stored and to carry out again a repeated formation of hash function values starting from this starting value m_0 after each activation of the key and to repeat this formation successively one time less in each case and then to feed the respective final value directly into the buffer 4. Any other distributions are equally possible, e.g. logarithmic sample selection.

This terminates the preparatory operations for starting up normal authentication operation with the vehicle security device. Such an authentication attempt with which a user attempts to demonstrate to the vehicle his authorization for use, thus opening the vehicle and cancelling the disabling facility which is set when the vehicle is parked is explained. Such an authentication process is initiated by actuating the starting button 6 of a key unit 1, the starting signal S_{ST} which is thus generated causing the inverse value m_i which is instantaneously present in the buffer 4 to be read out, the said inverse value m_i being subsequently passed on together with the key-end identification data ID_S as user code information M to the transmitter 5 and fed from there via the infrared transmission link 9 to the vehicle-end receiver 10. Here, the identification data information ID_S is initially extracted from the user code information M in the locking control 2 and compared with the vehicle-end identification data ID_K. If the required hardware identity, which is tested in this way, of a key 1 which is intended for the vehicle is not present, the user code information M is prevented from being passed onto the CAN bus and from there to the further pieces of control equipment with an item of corresponding control information to the gate function block 13, and the authentication process is aborted without the vehicle being unlocked or the disabling facility being cancelled. Otherwise, the function code information is subsequently interrogated as to whether a normal authentication process or a diagnostic process, for example for dealing with faults, is present.

If a normal identification-tested authentication attempt occur, the transmitted inverse value m_i is passed on as a component of the transmitted user code information M from the locking control via the CAN bus to all the control devices 2 involved in the process and fed there in each case to the unit 14 for generating hash function values and to the gate 15. The unit 14 for generating hash function values calculates the hash function value m′ which is associated with the fed-in inverse value m_i and passes this on as actual authorization information m′ to the comparator 17 and to the second gate 18. In the meantime, the associated key number ID_j is determined using the identification data ID_S contained in the user code information M and the value $[m_{i+1}]$ stored in the associated memory location of the desired authorization information memory 16 is read out to the other input of the comparator 17, this value $[m_{i+1}]$ corresponding to the inverse value information which is fed to the control device 2 during the last authentication to be carried out successfully with this key unit 1. If the comparator 17 detects correspondence of the actual authorization information and desired authorization information $[m'=m_{i+1}]$, it generates the use-enabling signal S_F which on the one hand as a control signal fed back to the gate 15 triggers the overwriting of the respective memory location by the inverse value m_i fed in during this authentication and on the other hand brings about, together with the use-enabling information generated simultaneously in the other control devices involved in the process, the entire cancelling of the electronic disabling facility in that all the control devices are restored to their operational state. If it is intended to save memory space in some of the pieces of equipment, there may be provision for only a portion, e.g. 2 bytes, of the entire desired authorization information $[m_{i+1}]$ to be stored in the said pieces of equipment and to compare only this portion with the corresponding portion of the hash function value m′ in the comparator block 17. So that, nevertheless, faulty deactivation of the disabling facility can be prevented, which could otherwise occur because of the reduced comparison particularly with a large capture range, for at least one piece of equipment, for example the locking control device, the complete code comparison is retained, the result of which is transmitted to the devices with shortened comparison, the generation there of the use-enabling information being associated with the presence of a positive result of the complete code comparison.

On the other hand, if the comparator function block 17 detects non-correspondence, provided that the number of successive non-correspondences has not yet exceeded the capture range by a number N if possible repetitions it transmits a non-correspondence signal N_U to the gate 18 which in response feeds back the hash function value m′ generated at the device end to the input side of the unit 14 which generated hash function values, after which the latter carries out a renewed formation of hash function values using this input value m′, the result of which formation of hash function value is then transmitted to the comparator 17 as a new actual authorization information. This recursive generation of hash function values is continued until either the comparator 17 detects correspondence of one of the successively generated items of actual authorization information with the desired authorization information $[m_{i+1}]$ present, after which, as stated above, generation is continued or the loop repetition number has reached the maximum number N, for example equal to the power n of a series of hash function values, prescribed by the capture range, after which the authentication process is aborted as unauthorized and the disabling facility continues to be activated or a new item of user code information with correct identification data arrives, after which the loop counter is reset and the generation of hash function values is continued with the newly transmitted inverse value.

As already stated in brief above, the capture range serves to restore synchronization of the key end and vehicle end which have become out of step as a result of single or multiple actuation of the key without reception contact of the vehicle end for the associated transmission protocol in that the vehicle end is readjusted to the inverse value which is now present in the key 1 by means of correspondingly frequent, successive formation of hash function values with the capture range. If the capture range N is selected to be exactly as large as the power N of the sequence of inverse values, the synchronization before an authorizing key can always be restored. By virtue of the property, typical for hash function values, that the said function values are assumed to be distributed virtually with identical probability over the entire value range, and by virtue of the fact even when a reduced algorithm with 8-byte values is used 10^{20} function values are possible, it is extremely improbable, even with a capture range of $N=10^5$ that an unauthorized person, even if he were to have somehow overcome the identification test, would achieve positive authentication by transmitting inverse function values on a trial and error basis using the capture range, in which case it would be possible to prevent frequent attempts of this kind by means of a corresponding time window or limit on the number of attempts within which an authorizing authentication would have to take place, while otherwise the vehicle would continue to be disabled in response to further authentication attempts, it being possible for such disablement to be cancelled for example only by the vehicle manufacturer via the diagnosis 19. Of course, the mode of operation of the vehicle security device proceeds in an analogous fashion for any other authentication process desired for the said device or for other key units as described above.

The selection of the capture range N=n which is the same size as the power of the inverse value sequence n also provides a very convenient way of producing a replacement key. As mentioned above, the inverse starting value m_0 was originally generated at the key manufacturer's SH by the repeated formation of hash function values from a key-specific initial random value r_0, for example by application Times, i.e. $m_0 = = H^T[r_0]$ where for example T = 400,000. If a replacement key is to be provided, it is initialized at the key manufacturers' SH, as was the original key, with the exception that the value $m_0{'} = H^{T-N}[r_0]$ is selected starting from the same initial random value r_0 as inverse starting value $m_0{'}$. Now, an authentication dialogue with the vehicle is carried out using this replacement key. The replacement key firstly transmits the value $x = H[m'_{n-1}] = H^{n-1}[m_0{'}] = H^{T-1}[r_0]$ to the vehicle. However, this value lies with certainty in the capture range of the vehicle end since it follows from this that:
$H^N x = H^{T+N-1}[r_0] = H^{N-1}[m_0]$.

The replacement key is automatically interpreted by the first authentication dialogue via the capture range as an authorizing key, as a result of which the instantaneously transmitted value X is automatically transferred into the vehicle-end design authorization information memory 16. This in turn simultaneously makes the original key automatically invalid since its values lie with certainty outside the capture range of the new inverse value x. A separate disabling process for the original key which has for example been lost is therefore unnecessary. With this procedure, a number T/N of replacement keys can be successively authenticated; as a concrete example when T =

400,000 and N=n=100,000 four keys which can be replaced one after the other and have the same key number are obtained. Of course, depending on requirements, an alternative way of implementing replacement keys in this field can be realized by using an additionally encryption method, for example, the asymmetrical RSa signature method known in cryptography [described in Annex C of ISO/IEC JTC1/SC20/WG N115, DIS 9594-8, Gloucester, Nov. 1987 or the asymmetrical DES/data encryption standard] method, in particular if the capture range is selected to be smaller than the power of the inverse value sequence and therefore the above technique for implementing replacement keys is not possible. Furthermore, implementation of replacement key may be achieved by means of the diagnostic interface and the special function memory 20.

Consequently, the vehicle security device shown provides security against a vehicle being used by third parties without authorization in a way which involves little outlay, provides a relatively high degree of protection and enables in particular the protected storage of items of secret code information at the vehicle end to be dispensed with, which permits a plurality of pieces of vehicle equipment to be used without logistical security problems. Furthermore, costly bidirectional data communication between the key end and vehicle end is not absolutely necessary. Specifically, it is possible to claim that 64 bits are sufficient for the hush function code and therefore the transmission time and the computational outlay are significantly lower than in the case of an equally conceivable use of the RSA method which, as an asymmetrical encryption method, also only requires an item of secret information to be stored at one end but has a large word length of 512 bits and thus, in view of the computational capacities present in a vehicle, required long computational and transmission times.

It is self-evident that only the units and operations which are essential to the invention have been mentioned in the above example and further customary units and operational sequences are additionally provided, and that a person skilled in the art is capable of performing, within the scope of the invention, a plurality of modifications of this embodiment, for example using another one-way function, application-specific changes to the completely stated numerical examples, dispensing with the identification test or using a chip card system instead of the infrared signal transmission. Additionally, the invention can be realized as a system with bidirectional exchange of authentication data, in which for example an item of random numerical information is transmitted from the vehicle to the key unit and transmitted by XOR linked to the inverse value information and is compared for correspondence. An embodiment of this kind prevents an unauthorized person who during temporary possession of an authorizing key produces successive user code information from it from successfully obtaining authentication with respect to the vehicle using this false key.

Claims

1. A vehicle security device with electronic use-authorization coding, having

- a user-end key unit for successfully transmitting items of user code information which differ from one another,
- a vehicle-end piece of equipment for receiving the user code information which is transmitted respectively by a key unit, for determining an item of actual authorization information which is dependent on the received user code information and comparing it with an item of desired authorization information which is present at the vehicle end and for generating, in a comparison-dependent way, an item of use-enabling information, wherein:
- the successively transmitted user code information contains an inverse value for a one-way function,
- the desired authorization information is in each case the one-way function value of the inverse value contained in an item of associated user code information and
- the determination of the actual authorization information from the received user code information includes the formation of the one-way function value of the inverse value contained in the received user code information.

2. A vehicle security device according to Claim 1, wherein

- the successively transmitted inverse images constitute a sequence which results from repeated application of the one-way function, these inverse images being used in reverse order with respect to the sequence formation to form the successive items of the user code information, and
- the desired authorization information consists in each case of that inverse image which was transmitted with

the user code information during the use-authorization testing process which the last time proceeded positively with this key unit.

3. A vehicle security device according to Claim 2, wherein selected sequence elements of sequence are stored as samples, and a respective instantaneous subsequence between two samples is stored, in an inverse image memory of the key unit, a subsequent instantaneous subsequence being respectively generated then as the latest and stored instead of the previous one when the last inverse image of the previously subsequence has been transmitted.

4. A vehicle security device according to Claim 2 or 3, wherein an item of new actual authorization information is determined as a one-way function value of the previous actual authorization information after a respective negative result of the comparison of actual authorization information and desired authorization information for a prescribed maximum number of repetitions and the said new actual authorization information is compared with the desired authorization information.

5. A vehicle security device according to any one of Claims 2 to 4, wherein replacement key units which can be used successively for the key unit are provided, the inverse images of one key unit which can be subsequently used forming a subsequence which lies directly in front of the inverse image subsequence, of an entire sequence which is generated by repeated formation of one-way function values starting from a starting value which is stored centrally on a key number-specific basis.

6. A vehicle security device according to any one of Claims 1 to 5, wherein a cryptographic hash function is used as one-way function.

7. A vehicle security device according to claim 6, wherein the cryptographic hash function is the RIPEMD function.

8. A vehicle security device according to any one of Claims 1 to 7, wherein a plurality of vehicle-end pieces of equipment is arranged in parallel to determine the respective actual authorization information from an item of received user code information and to compare the same with the desired authorization information and to generate, as a function of the comparison, an item of use-enabling information.

9. A vehicle security device according to any one of Claims 1 to 8, wherein a locking control device of the vehicle forms a vehicle-end piece of equipment of the security device.

10. A vehicle security device according to any one of Claims 1 to 9, wherein

- the respectively transmitted user code information contains an item of vehicle-specific and an item of key-specific identification information and
- the identification information of an item of received user code information can be evaluated in advance in a vehicle-end piece of equipment, the use-authorization testing process being aborted after non-authorizing transmitted identification data are detected.

11. A vehicle security device according to any one of Claims 1 to 10, wherein

- a plurality of authorizing, user-side key units are provided for a vehicle, which key units transmit different inverse image sequences,
- the transmitted user code information each containing an item of key identification information and
- an item of specific desired authorization information

being capable of being stored in, and read out of, a memory, which can be addressed with the aid of the key identification information, in each vehicle-end piece of equipment involved in the process for each key unit.

12. A vehicle security device with electronic use-authorization coding, substantially as described herein with reference to and as illustrated in the accompanying drawing.

Patents Act 1977
Examiner's report to the Comptroller under Section 17
(e Search report)

Application number
GB 9506279·0

Relevant Technical Fields

(i) UK Cl (Ed.N) G4H (HTG)

(ii) Int Cl (Ed.6) B60R, E05B

Search Examiner
M J DAVIS

Date of completion of Search
7 JUNE 1995

Databases (see below)
(i) UK Patent Office collections of GB, EP, WO and US patent specifications.

(ii) ONLINE: WPI

Documents considered relevant following a search in respect of Claims :-
1-12

Categories of documents

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

Category	Identity of document and relevant passages	Relevant to claim(s)
A,E	GB 2282687 A (BRITISH TECHNOLOGY GROUP) eg Abstract	

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).