(12) UK Patent Application (19) GB (11) 2 282 687 (13) A

(43) Date of A Publication 12.04.1995

(21) Application No 9420363.5

(22) Date of Filing 10.10.1994

(30) Priority Data
(31) 9320767 (32) 08.10.1993 (33) GB

(51) INT CL[6]
B60R 25/00

(52) UK CL (Edition N)
G4H HTG H13D H14A H14D
U1S S1820 S1824 S1831 S1834 S1839

(56) Documents Cited
None

(58) Field of Search
UK CL (Edition M) E2A ALV , G4H HTG
INT CL[5] B60R

(71) Applicant(s)
British Technology Group Limited

(Incorporated in the United Kingdom)

101 Newington Causeway, LONDON, SE1 6BU, United Kingdom

(72) Inventor(s)
Thomas Mark Angus Lomas

(74) Agent and/or Address for Service
D R Chandler
British Technology Group plc, 101 Newington Causeway, LONDON, SE1 6BU, United Kingdom

(54) Vehicle security

(57) In a vehicle security arrangement including a first part P1 for incorporation in a vehicle and a second part P2 for use as a key to allow operation of the vehicle, both the first part and the second part include signal processing means SP1, SP2 and signal receiving and sending means Rx1, Rx2, Tx1, Tx2, the signal processing means being responsive to an input signal of a first value to generate an output signal of a second value in accordance with a one-way hash function performed with a stored value SV on the first value, the stored value being computationally unfeasible to determine from the first and second values, the first part P1 including means to produce a first value signal V1 and in operation send this first value signal for the second part P2, in operation in the key position for the vehicle, to receive as a said input signal therefor and form a said second value output signal V2 therefrom, the first part P1 also including means Rx1 to receive said output signal of the second part P2 sent therefrom together with means CM to compare the received said output signal with a check value generated from the produced first value by the signal processing means SP1 of the first part and permit or prevent operation of the vehicle in accordance with the result of the comparison following the signal exchange.

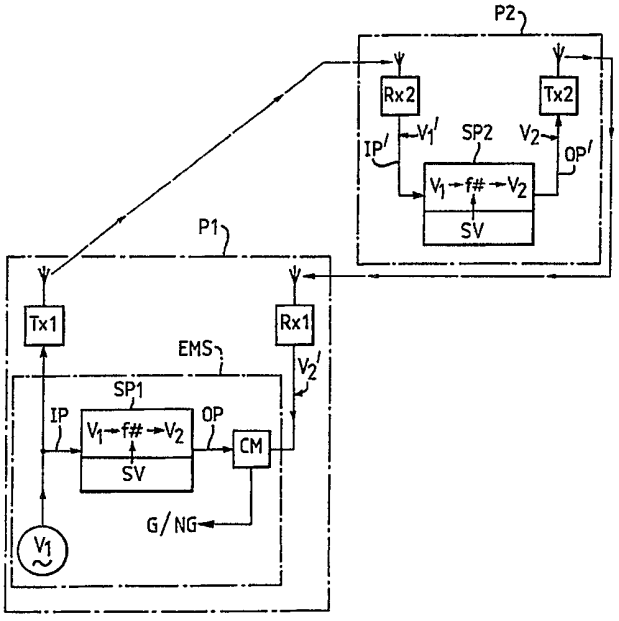

Fig. 2

GB 2 282 687 A

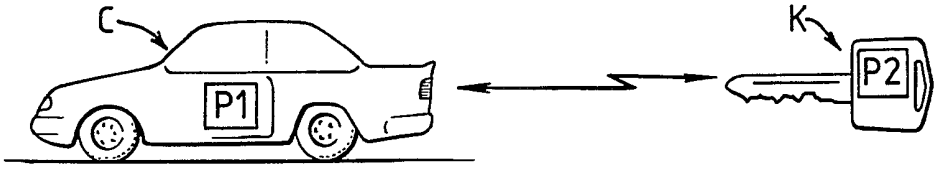
C
P1
K
P2

Fig.1

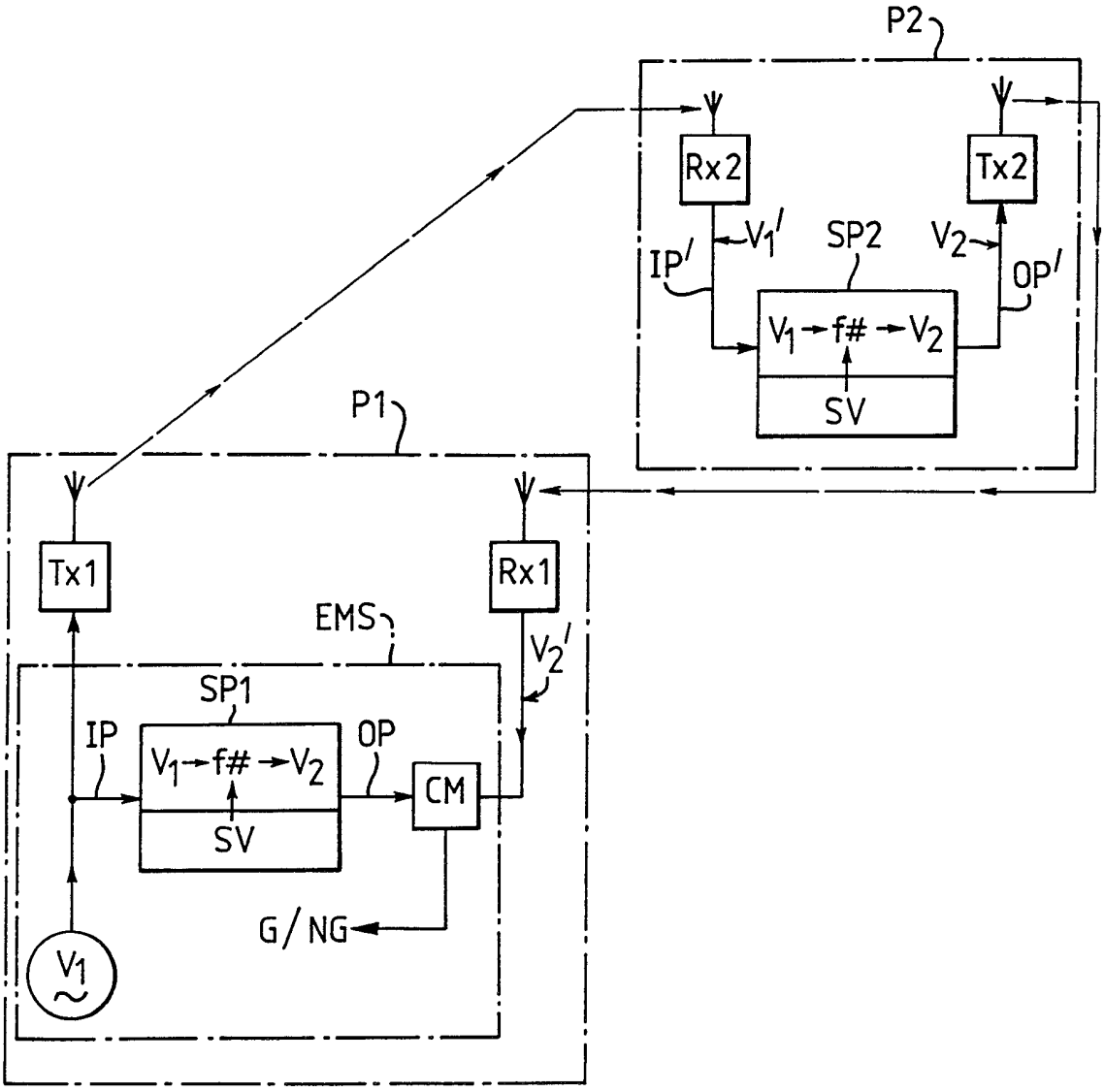
P2
Rx2
Tx2
IP'
V1'
SP2
V2
OP'
V1 → f# → V2
SV
P1
Tx1
Rx1
EMS
V2'
SP1
IP
V1 → f# → V2
OP
CM
SV
G / NG
V1

Fig. 2

2282687

VEHICLE SECURITY

This invention relates to the improvement of the protection of vehicles against theft or other unauthorised use.

The protection of a vehicle against theft and other unauthorised use has developed from simple door locks and keys on the doors to extensive systems of sensors based on ultrasonics, microwaves, vehicle voltage change or vibration which cause an alarm to be sounded. Complicated door locks and keys resist unauthorised entry and a lock is used on the steering column. Theft by driving away of a car after "hot-wiring" to bypass switches in the ignition circuit is still frequent despite these precautions.

The cost of precautions against theft and the insurance claims for stolen vehicles is now so large as to be of great concern to insurers and the motor industry, also significantly increasing insurance costs.

There is a great need for an effective technique for the protection of a vehicle against unauthorised removal or use, that is theft in general terms, which does not make authorised use of a vehicle too cumbersome.

It is an object of the invention to provide a vehicle security arrangement effective to immobilize a vehicle apart from authorised use which arrangement is not obstructive of authorised use.

According to the invention there is provided a vehicle security arrangement including a first part for incorporation in a vehicle and a second part for use as a key to allow operation of the vehicle, in which arrangement both the first part and the second part include signal processing means and signal receiving and sending means, the signal processing means being responsive to an input signal of a first value to generate an output signal of a second value in accordance with a one-way hash function performed with a stored value on the first value, the stored value being computationally unfeasible to determine from the

first and second values, the first part including means to produce a first value signal and in operation send this first value signal for the second part in operation in the key position for the vehicle, to receive as a said input signal therefor and form a said second value output signal therefrom, the first part also including means to receive said output signal of the second part sent therefrom together with means to compare the received said output signal with a check value generated from the produced first value by the signal processing means of the first part and permit or prevent operation of the vehicle in accordance with the result of the comparison following the signal exchange.

The first part may be incorporated in a vehicle part vital to the integrity or operation of the vehicle. The vehicle part may be the engine management device.

The one-way hash function may be of the American Secure Hash Standard type, abbreviated as SHS.

The arrangement may generate a fresh first value at least on each use of the second part with the first part. The fresh value may be unpredictable. The stored value may be held concealed. The stored value and the first value may, when concatenated, exceed three hundred bits.

According to a further aspect of the invention there is provided a lock and key method of vehicle security including causing the lock to provide an identical first value to both the lock and the key, storing in the lock and the key an identical concealed value, causing or permitting the lock and the key to separately calculate in an identical manner from their respective first and second stored values an output value, returning the output value of the key calculation to the lock, comparing the output values to permit enabling of the lock on satisfactory comparison, the stored concealed value being computationally infeasible to determine from the first or output values.

According to another aspect of the invention there is provided a method of providing vehicle security including providing a source of a first signal value, providing first and second one way hash function signal processors each having the same concealed stored value, positioning said first processor on a vehicle to be provided with security, positioning said second processor on a key to said vehicle, connecting said source to said first processor and linking said source to said second processor to permit the performance of the hash function in both processors to produce respective outputs providing comparator means connected to the first processor and linked to the second processor to compare the outputs to produce a vehicle-enabling output on satisfactory comparison.

Embodiments of the invention will now be described with reference to the drawing said by way of examples including that of a lock and key for a vehicle.

In the drawings Figure 1 is a schematic of the security arrangement for a passenger car and Figure 2 shows in more detail parts of the arrangement in Figure 1.

In this document the term vehicle V includes but is not limited to cars, lorries, trains, boats and aircraft.

A key K for an arrangement exemplifying the invention includes in a portion P2 of the arrangement a computation device, such as a microchip SP2, with an appropriate in-built power source or means to receive power from an external source (not shown). The computation device is formed to perform a one-way hash function F# on a supplied signal value V_1' at input IP' and also contain a concealed secret stored value SV as the source of the other value for performance of the hash function. The key also includes means Rx2 for the reception of a signal value V_1' as the supplied value for performance of the hash function. The means for reception may be direct connection, by electrical contacts, or indirect connection, for example by magnetic coupling, electromagnetic radiation and other techniques. The key also includes means for transmission Tx2 of the result V_2 of the hash function from the output OP' of device SP2.

The key of the arrangement is for co-operative use with a lock of the arrangement, for example the lock receives the key. The lock includes appropriate transmission Tx1 and reception Rx1 means for use with the key. The lock supplies to the key the above-mentioned supplied value, which value is produced in a further portion P1 of the arrangement for supply to the lock and is preferably a fresh and unpredictable value V_1 at each use. Preferably the further portion is incorporated in the vehicle engine management system EMS so as not to be removable or interrogated without destruction or disabling damage. The further portion includes a computation device SP1 to perform the one-way hash function on the value V_1 supplied at input IP and contains the identical stored valued SV concealed therein. The key transmits the result V_2 of the hash function to the lock via Rx1 for application, V_2', to the further portion and comparison CM with a check value at output OP of device SP1, the result of the hash function applied in the further portion to the identical stored value SV and the supplied value V_1. A satisfactory result G of the comparison will allow the use of the vehicle. The turning of the key in the lock may be prevented until the satisfactory result or may be permitted to a certain amount thereuntil, a satisfactory result then permitting operation of the engine management system. A failure of the comparison is indicated as an inhibition of use, NG.

Various one-way hash functions are known and may be used, provided the requirement of computational unfeasibility is met. One example is the American Secure Hash Standard (SHS) originally intended for e-mail message signing. The generated and stored values are concatenated and the SHS applied to the result. Provided the sum of the lengths of the values is large enough, typically some 380 bits, the result is effective for the "question-and-answer" exchange. Details of the SHS are given in Federal Information Processing Standards Publication: "Secure Hash Standard" Draft, National Institute of Standards and Technology, January 22, 1992.

In an exemplary installation in a private car the lock is on the steering column as at present and the further portion to produce the supplied value is included in the engine management system computer. The connections to the key are by electrical contacts. These contacts transfer signals and, if required, power for the computation device in the key. On introducing the key into the lock the produced value is provided to the key where the one-way hash function is performed using the stored value and the result returned via the lock to the engine management system computer. Here the received result is compared with the result of the local performance of the one-way hash function on the stored value and the produced value. If the results of the "question-and-answer" exchange match the key has operated the lock and the vehicle can be put into use. If the results do not match the vehicle remains immobilized. If required the engine management can be inhibited, alternatively or additionally the steering lock can be kept locked.

To summarise the exemplary arrangement described an unpredictable value V_1 generated in the part P1 is supplied both for transmission to part P2 and as an input IP to the hash function computation device SP1, the other input to which is stored value SV, where output OP is calculated in accordance with the hash function. The value V_1 transmitted to part P2 is received and supplied as the same value, but identified as V_1' for convenience, as input IP' to computation device SP2 where the same hash function calculation using also stored value SV is performed to produce an output OP of value V_2. Outputs OP and OP' should have the same value. Value V_2 is transmitted to part P1 for comparison, as value V_2', with OP in a comparison means CM. If the comparison is satisfactory enabling output G is produced, if not the inhibiting output NG is produced. Conveniently a portion of part P1 is in the engine management system EMS.

The key cannot be duplicated without knowledge of the hash function and the concealed stored secret value. This would incur considerable expense, even if possible. Similarly the engine management system further portion could not be imitated easily.

The arrangement described is not susceptible to being breached by "capturing" one sequence of question-and-answer and replaying it later when the other vlue is a fresh and unpredictable one.

Clearly the engine management system is not the only element of the vehicle which could be used, the fuel supply or starter motor could include a device to inhibit its operation.

If required the question-and-answer sequence could be repeated at intervals during use of the vehicle to prevent attempts to defeat the security arrangement by bypassing the lock once the vehicle has started.

The invention also provides a checking arrangement. If a key which operates a vehicle is to be checked as the correct one, for example to defeat change of engine management computer and key and lock in a stolen vehicle, the checking arrangement is used. The key is placed in the arrangement and the arrangement causes the key to calculate a value. The manufacturer of the vehicle has a record of the correct value for a specific Vehicle Identification Number and on approved request provides this for comparison with the calculated value as a check on the correctness of the key for the vehicle, without the concealed stored value being revealed.

Tight security of the keys and other components by the manufacturer is important. A supply of pairs of "chips", each pair holding an identical secret stored value, is needed but this is not a serious problem if "burn-in" techniques are used to insert the stored value. "Chips" can also be provided in sets of more than two to permit more than one authorised user.

It is not essential that the second part, that for use as a key, is of conventional key form nor that a conventional lock for the key be provided. The arrangement may be of "wireless" form using for example visible light, infra red, radio or other transmission methods. The key may be of "lay-on" form and not actually inserted in the lock. Power-supply may be of any suitable form. The key may have a rechargeable battery charged by inductive or other direct or indirect means. Solar energisation or recharging is also possible. The part of the arrangement in the vehicle may include suitable power back-up to cope with vehicle battery failure or removal and to help resist attempts to interfere with the proper operation of the arrangement.

To permit multiple authorised users a suitable number of chips, not just a pair, may be provided by the manufacturer to provide extra keys for delivery with a new vehicle. Clearly the users must ensure that the keys are not acquired by unauthorised users.

Suitable circuits and components for the production of arrangements according to the invention for a particular construction will be apparent to those skilled in the art, as with transmission/reception procedures to avoid break-through, cross-talk and other other-interference problems.

The techniques described above provide a vehicle security arrangement which is of little inconvenience to an authorised user while providing great deterrent to unauthorised use or theft of the vehicle. Even if a vehicle is stolen by towing or placing on a trailer the need to replace the engine management system is a very significant problem and makes profitable disposal very difficult.

CLAIMS

1. A vehicle security arrangement including a first part for incorporation in a vehicle and a second part for use as a key to allow operation of the vehicle, in which arrangement both the first part and the second part include signal processing means and signal receiving and sending means, the signal processing means being responsive to an input signal of a first value to generate an output signal of a second value in accordance with a one-way hash function performed with a stored value on the first value, the stored value being computationally unfeasible to determine from the first and second values, the first part including means to produce a first value signal and in operation send this first value signal for the second part, in operation in the key position for the vehicle, to receive as a said input signal therefor and form a said second value output signal therefrom, the first part also including means to receive said output signal of the second part sent therefrom together with means to compare the received said output signal with a check value generated from the produced first value by the signal processing means of the first part and permit or prevent operation of the vehicle in accordance with the result of the comparison following the signal exchange.

2. An arrangement according to Claim 1 in which the first part is incorporated in a vehicle part vital to the integrity or operation of the vehicle.

3. An arrangement according to Claim 2 in which the vehicle part is the engine management device.

4. An arrangement according to Claim 1 in which the one-way hash function is of the American Secure Hash Standard.

5. An arrangement according to Claim 1 to generate a fresh first value at least on each use of the second part with the first part.

6. An arrangement according to Claim 2 in which the fresh value is unpredictable.

7. An arrangement according to Claim 2 in which the stored value is held concealed.

8. An arrangement according to Claim 1 in which the stored value and the first value, when concatenated, exceed three hundred bits.

9. A lock and key method of vehicle security including causing the lock to provide an identical first value to both the lock and the key, storing in the lock and the key an identical concealed value, causing or permitting the lock and the key to separately calculate in an identical manner from their respective first and stored values an output value, returning the output value of the key calculation to the lock, comparing the output values to permit enabling of the lock on satisfactory comparison, the stored concealed value being computationally infeasible to determine from the first or output values.

10. A vehicle security arrangement substantially as herein described to the accompaniment of drawings.

Patents Act 1977
Examiner's report to the Comptroller under Section 17
(The Search report) -10-

Application number
GB 9420363.5

Relevant Technical Fields

(i) UK Cl (Ed.M) G4H (HTG), E2A (ALV)

(ii) Int Cl (Ed.5) B60R

Search Examiner
M J DAVIS

Date of completion of Search
1 NOVEMBER 1994

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

(ii)

Documents considered relevant following a search in respect of Claims :-
1-10

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family; corresponding document.

Category	Identity of document and relevant passages	Relevant to claim(s)
	NONE	

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).