Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2764412 C 2017/10/24

(11)(21) **2 764 412**

(12) BREVET CANADIEN / CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2010/03/26
(87) **Date publication PCT/PCT Publication Date:** 2010/12/16
(45) **Date de délivrance/Issue Date:** 2017/10/24
(85) **Entrée phase nationale/National Entry:** 2011/12/02
(86) **N° demande PCT/PCT Application No.:** EP 2010/054015
(87) **N° publication PCT/PCT Publication No.:** 2010/142474
(30) **Priorité/Priority:** 2009/06/10 (IT PN2009A000038)

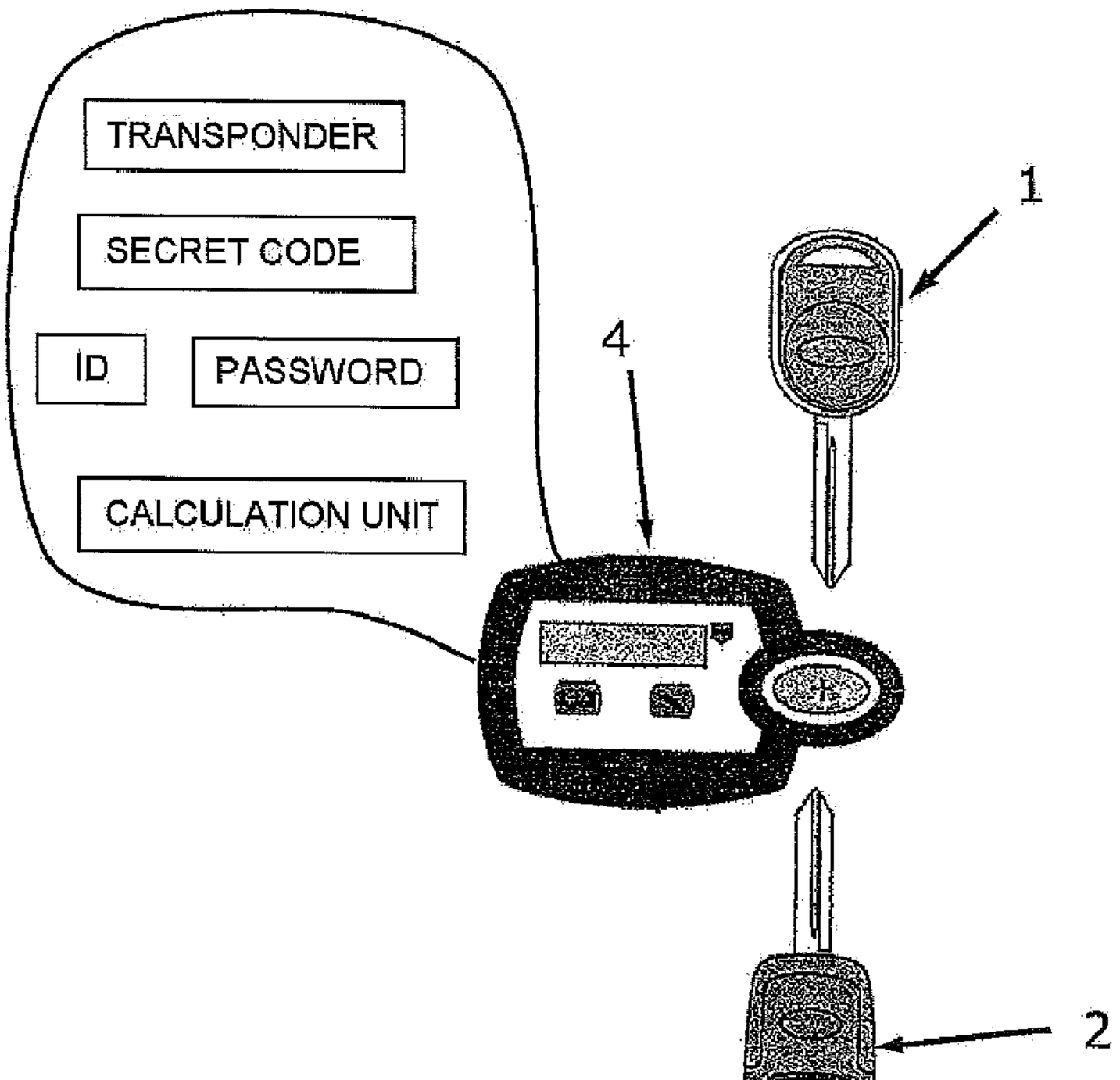
(51) **Cl.Int./Int.Cl.** ***G07C 9/00*** (2006.01), ***B60R 25/00*** (2013.01)

(72) **Inventeur/Inventor:**
REBULI, DAVID, IT

(73) **Propriétaire/Owner:**
KEYLINE S.P.A., IT

(74) **Agent:** GOUDREAU GAGE DUBUC

(54) **Titre : MOYEN DE REPRODUCTION POUR CLE A CODAGE ELECTRONIQUE ET PROCEDE ASSOCIE**
(54) **Title: DUPLICATION MEANS FOR AN ELECTRONICALLY CODED KEY AND RELATED METHOD**



(57) **Abrégé/Abstract:**
Method for the duplication of original electronic keys used in the automotive transports, and provided with coded and encrypted electronic authentication means, comprising: an Identification Code (ID), an encrypted secret code, a Password, an algorithm, data

CA 2764412 C 2017/10/24

(11)(21) **2 764 412**

(13) **C**

(57) **Abrégé(suite)/Abstract(continued):**
storage and computing means, able of being used in vehicles provided with a central processing unit able of storing an Identification Code (ID), an encrypted secret code, a Password, an algorithm, said duplication method being able of obtaining a duplicated key based on a blank key, which is originally provided with an algorithm, data storage means able of storing said Identification Code (ID), said secret code and said Password, wherein said data storage means are initially empty; said duplication is based on a duplication means and on a method which allows of using the blank key as intercepting means of secret codes sent by the vehicle central processing unit, and of transferring said information to the duplication means itself.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 December 2010 (16.12.2010)

PCT

(10) International Publication Number
WO 2010/142474 A1

(51) International Patent Classification:
G07C 9/00 (2006.01) *B60R 25/00* (2006.01)

(21) International Application Number:
PCT/EP2010/054015

(22) International Filing Date:
26 March 2010 (26.03.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PN2009A000038 10 June 2009 (10.06.2009) IT

(71) Applicant *(for all designated States except US)*: **KEY-LINE S.P.A.** [IT/IT]; Via Camillo Bianchi 2, I-31015 Conegliano (TV) (IT).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **REBULI, David** [IT/IT]; Via Camillo Bianchi 2, c/o Keyline S.p.A., I-31015 Conegliano (TV) (IT).

(74) Agent: **GIUGNI, Valter**; Via della Colonna 35, I-33170 Pordenone (IT).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) **Title**: DUPLICATION MEANS FOR AN ELECTRONICALLY CODED KEY AND RELATED METHOD

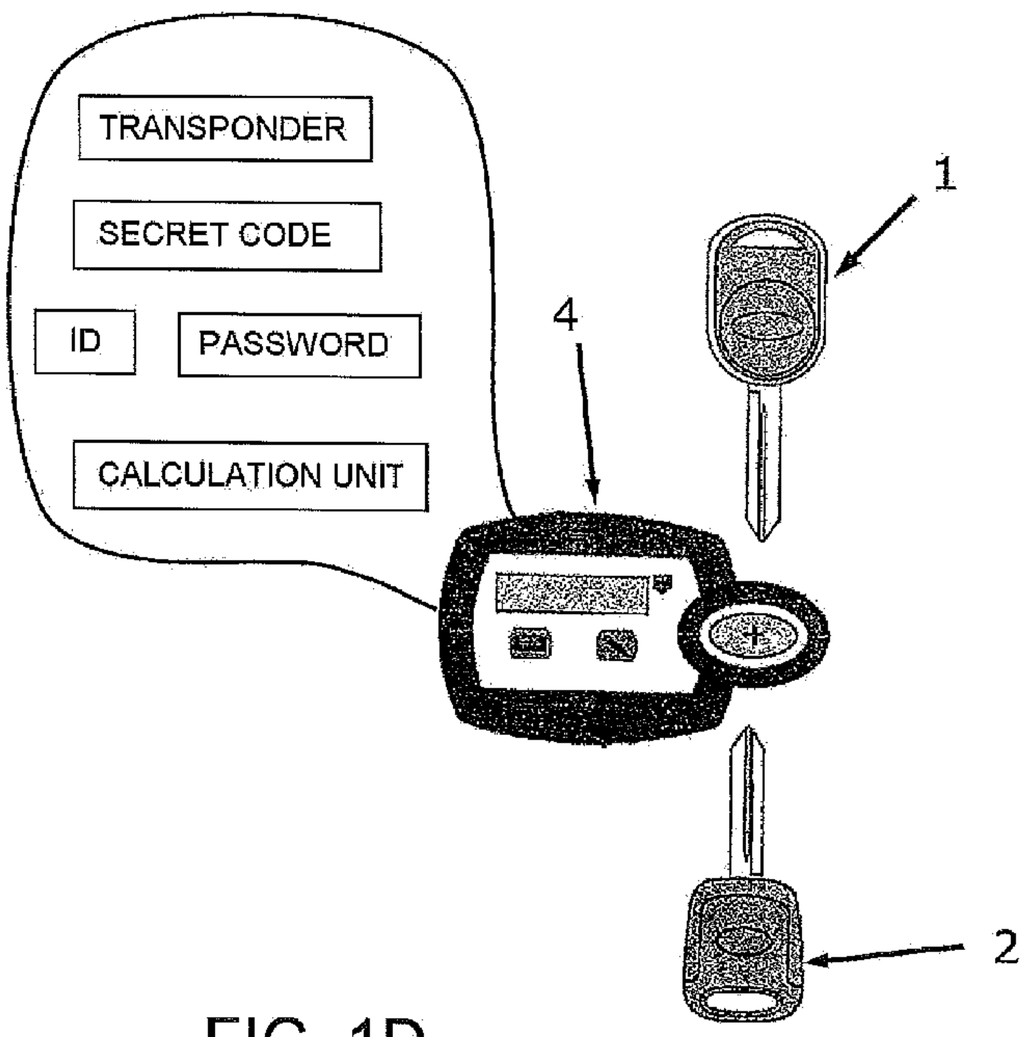


FIG. 1D

(57) **Abstract**: Method for the duplication of original electronic keys used in the automotive transports, and provided with coded and encrypted electronic authentication means, comprising: an Identification Code (ID), an encrypted secret code, a Password, an algorithm, data storage and computing means, able of being used in vehicles provided with a central processing unit able of storing an Identification Code (ID), an encrypted secret code, a Password, an algorithm, said duplication method being able of obtaining a duplicated key based on a blank key, which is originally provided with an algorithm, data storage means able of storing said Identification Code (ID), said secret code and said Password, wherein said data storage means are initially empty; said duplication is based on a duplication means and on a method which allows of using the blank key as intercepting means of secret codes sent by the vehicle central processing unit, and of transferring said information to the duplication means itself.

WO 2010/142474 A1

DUPLICATION MEANS FOR AN ELECTRONICALLY CODED KEY AND RELATED METHOD

DESCRIPTION

[0001] This invention refers to some means able of duplicating keys provided with both a mechanical code, of the conventional type, and of an electronic code, also in se known and employed for years in several technical applications.

[0002] The invention also refers to some methods in order to use said means and which allows the duplication of one of these keys.

[0003] In the following of this description, and in the attached claims, it will be specifically referred to the mechanical and electronic keys used in the nowadays produced vehicles, but it is intended that the invention applies also in different fields, as for instance in the armoured door, a safe etc ., provided a key with a double mechanical and electronic code, a respective lock and a related electronic central unit able of processing the data stored into the electronic codes of the key to be duplicated, and transmitted by it, is used. Moreover it is stressed that, even if it will be useless to the man skilled in the art, the invention applies to a central processing units and electronic keys wherein, before the central unit to allow the operation of the various vehicle functions, a double and mutual authentication between the electronic key and the central unit mounted in the vehicle itself is implemented. The means and the method of said mutual authentication are broadly described in the patent US 7,387,235 B2: "MUTUAL AUTHENTICATION SECURITY SYSTEM WITH RECOVERY FROM PARTIAL PROGRAMMING", assigned to Lear Corporation.

[0004] For this reason, in fact, the original key, and therefore the duplicated one, are provided with a double code for the reciprocal authentication, one being called «Secret code», and the other called «Password».

[0005] In fact, one of said codes is used by the central unit to authenticate the original key, and the second code is used by the original key to authenticate the central unit.

[0006] Furthermore, in order to more easily introduce the person skilled in the art into the field and technique of electronic keys with mutual authentication, reference is made to Fig. 6 of the above prior patent, which shows a method of mutual authentication between an electronic key and a respective central unit, which is activated when the key is inserted in its lock and turned until a suitable «start» signal is sent to the central unit itself. On this basis, the person skilled in the art is able to identify the technique field involved, and to easily understand its innovation with respect to said technique field.

[0007] It is known that when one wishes, or needs to duplicate, in a legal way, a mechanical or electronic key as described, several aspects have to be evaluated.

[0008] One aspect regards the time-length and the cost required for the key duplication activity; usually the duplication request is urgent as the user has lost one of its keys, or has to provide one or more extra keys to trustworthy people, such as relatives, assistants etc.

[0009] Another aspect refers to the practicality and actual feasibility of the duplication operation. In particular, it is advantageous that the duplication activity be available in a indeterminate plurality of different stations for key duplication, preferably well spread throughout the territory where the vehicle usually travels, so that the user who wishes to duplicate a key may easily and quickly access a station and obtain the required duplicated key, which must therefore be delivered to the station itself.

[0010] Various methods and means are known, which allow the duplication of electronic keys; such means and methods are extensively described in a number of patents, or related applications, among these we here cite:

US 5,838,251 A, US 2004/078563 A1,
EP 1 339 024 A,
WO 2006/032354,
GB 2 340 644 A,
PCT/EP2007/060856, (of the same applicant), US 2001/049066 A1.

[0011] All of these means and methods require, to duplicate an electronically coded key, a unique storing and processing center of a large quantity of keys of the considered type, and of the transmission means, typically on-line (internet), which are used to transmit and receive information from a local station that has to physically generate and deliver the duplicated key, and to which the client addresses, towards and from such storing, processing and coding/decoding center.

[0012] The teaching and the information presented in the above documents can be generally well implemented, and some are actually realized.

[0013] However all of them show a common drawback which limits the operability and the quickness, and makes them less operable. This common drawback consists in that the key duplication requires:

a) the availability of a typically remote center, able to receive, process and generate the required codes to make out the required key, and

b) telecommunication means to transmit and receive the coded data, from the local station to said processing center, and vice-versa.

[0014] Such requirements obviously imply the existence and the correct operation of a specific organization of trained and co-ordinated personnel and distributed on the territory, and of specific procedures which have to be carried out by said personnel both in the local station and in the processing center.

[0015] Obviously all that implies a higher operation complexity, organizational limits and so is less reliable and convenient for a user who only asks the duplication of its key, in an easy way and without depending on outer and far-away centers, and on transmission and receiving means for the coded data.

[0016] It is then desirable, and is an object of the preferred embodiment of the present invention, to perform a method for the duplication of electronic keys which eliminates the described drawbacks, is easily and safely usable and which can be carried out with prior means available.

[0017] This and further purposes are achieved by a method according to preferred embodiments of the invention.

[0018] In accordance with a first aspect of the present invention, there is provided a method for the duplication of original electronic keys, the method comprising:

intercepting a radio-electric interrogating signal of an encrypted electronic authentication system transmitted between a central processing unit of a vehicle and an original key, the radio-electric interrogating signal including therein an encrypted random code generated by an algorithm, the encrypted random code including therein a secret code, the encrypted electronic authentication system utilizing an identification code (ID), the secret code, a password, and the algorithm;

transferring said intercepted random code to a key duplicating device, the duplicating device having said algorithm installed thereon;

decrypting said secret code from said random code at said key duplicating device using said algorithm;

performing an interrogation process by transmitting a radio-electric signal, including said secret code, from said key duplicating device, to said original key;

receiving the password, transmitted by said original key, at said key duplicating device in response to the transmission of the secret code; and

transferring said password to a blank key, the blank key including the algorithm and a data storage device configured to store an identification code (ID), a secret code and a password.

[0019] In accordance with a second aspect of the preferred embodiment of the present invention, there is provided a method for the duplication of original electronic keys, comprising:

intercepting, via an interception device placed in proximity to an original key, at least one radio-electric signal containing an identification code (ID) and an encrypted random code and storing the intercepted identification code (ID) and the encrypted random code in a storage of the interception device, the radio-electric signal being generated by an electronic authentication system of a vehicle performing authentication by

transmitting, by a processing unit and in response to the activation of a central processing unit, the radio-electric signal including an identification request for the identification code (ID) of the original key, to the original key,

transmitting, from the original key, the identification code (ID) stored in the original key to the central processing unit,

comparing, at the central processing unit, the identification code (ID) with a previously stored corresponding ID code, and

in response to a positive result from the comparing, generating, at the central processing unit, a random code encrypted by an algorithm, which includes the secret code, and sending the random code to the original key;

transmitting, from an interception device to a duplicator device having said algorithm installed thereon, the intercepted identification code (ID) and the encrypted random code; and

decrypting, at the duplicator device and using said algorithm, said encrypted secret code from the encrypted random code.

[0020] In accordance with a third aspect of the present invention, there is provided a method for the duplication of original electronic keys, comprising:

a) interrogating an original key by transmitting a radio-electric signal from a key duplicating device to the original key inserted into the key duplicating device, the original key and key duplicating device including a common decrypting algorithm;

b) receiving a radio-electric signal from the original key containing an identification code (ID);

c) storing said identification code ID into a blank key;

d) receiving, at the blank key, in response to an attempt at ignition from the blank key inserted into a vehicle lock of a vehicle, and from a central processing unit of the vehicle, a radio-electric signal containing an encrypted secret code;

e) decrypting, at the key duplicating device, the secret code using said algorithm;

f) interrogating, at the key duplicating device, the original key with a radio-electric signal containing the secret code in order to emulate vehicle operation;

g) receiving, at the key duplicating device, a passcode from the original key in response to the interrogating;

h) transmitting, from the key duplicating device to the blank key, the passcode and the secret code; and

i) storing, into a defined memory of the blank key, the passcode and the secret code.

[0021] In accordance with a fourth aspect of the preferred embodiment of the present invention, there is provided a method of duplicating a motor vehicle electronic key, comprising:

transmitting to the motor vehicle electronic key, by a first device, an encrypted secret code;

receiving, by the motor vehicle electronic key, the encrypted secret code;

as the electronic key is receiving the secret code which has been encrypted, intercepting the transmission to the motor vehicle electronic key by the first device, comprising the encrypted secret code, and storing, by a second device different from the first device and different from the motor vehicle electronic key, the encrypted secret code, which is extracted from the transmission;

interrogating the motor vehicle electronic key, by a duplicator device which is different from the first device and different from the motor vehicle electronic key, using the encrypted secret code which has been intercepted and stored;

receiving, by the duplicator device from the motor vehicle electronic key, a password transmitted from the motor vehicle electronic key in response to the interrogating;

storing, by the duplicator device, the password transmitted from the motor vehicle electronic key;

transmitting, by the duplicator device, the password to a blank key; and

storing the password in the blank key.

[0022] In accordance with a fifth aspect of the present invention, there is provided a system for duplicating a motor vehicle electronic key which operates when there is a transmission to the motor vehicle electronic key, by a first device, an encrypted secret code and when there is a receiving, by the motor vehicle electronic key, the encrypted secret code, the system comprising:

a receiver which, as the motor vehicle electronic key is receiving the encrypted secret code, intercepts the transmission to the motor vehicle electronic key by the first device,

comprising the encrypted secret code, and stores the encrypted secret code, which is extracted from transmission;

a transmitter, which is part of a duplicator device and different from the first device, which interrogates the motor vehicle electronic key using the encrypted secret code which has been intercepted and stored;

a receiver, which is part of the duplicator device, which receives from the motor vehicle electronic key, a password transmitted from the motor vehicle electronic key in response to the interrogating;

a memory, within the duplicator device, which stores the password transmitted from the motor vehicle electronic key;

a transmitter, which is part of the duplicator device, which transmits the password to a blank key.

[0023] Unless the context clearly requires otherwise, throughout the description and the claims, the words “comprise”, “comprising”, and the like are to be construed in an inclusive sense as opposed to an exclusive or exhaustive sense; that is to say, in the sense of “including, but not limited to”.

[0024] Any discussion of the prior art throughout the specification should in no way be considered as an admission that such prior art is widely known or forms part of common general knowledge in the field.

[0025] Features and advantages of the embodiments of the invention will be apparent from the following description, as non-limiting example, with reference to the attached figures, wherein:

-Figures 1A, 1 B, 1 C represent respective means which have to be operated in the invention, and which show, in a simplified and symbolic way, their type and content both in the hardware and in the software, which take part to the invention method,

-Figures 1 E and 1 F show respectively, in a simplified form, the logical flowchart of the various devices comprised in the original key and in the vehicle central unit,

-Fig. 2 shows a flow-chart of the various steps of the method according to the principle of the invention,

-Fig. 3 shows a schematic of the relationship among the various steps of the method of Fig. 2, and of the relationship among the various means which take part in the method of the invention,

-Fig. 4 shows a flow-chart of the various steps of an improved embodiment of the method according to the invention,

-Fig. 5 shows a schematic of the relationship among the various steps of the method of Fig. 4, and of the relationships among the several means operating in each of said steps,

-Fig. 6 shows a logical and schematic flow-chart of the sequence of the functions and of the reciprocal relationships between an electronic key and the respective central unit, implemented to work at a «mutual authentication» mode,

[0026] With reference to the Figures from 1A to 1 D, the method of the invention uses the following means:

A) an original key 1, which has to be duplicated, and provided with:

- a first memory capable of storing a secret code, a Password and a first Identification code ID,
- a first transponder comprising a suitable algorithm,
- a logical or computing unit,
- further devices, per se generally known, which allow to transmit and to receive, modulate/de-modulate the radio-electric signals transmitted and received.

[0027] While the Figures from 1A to 1 D describe in a preferred way the content of the devices needed to the invention, Figure 1 E and 1 F in particular show the constructional and circuital content of the key and of the central unit installed into the vehicle, and which are needed to make the just cited devices to operate.

[0028] These devices are for long time mounted and working in the presently made vehicles, and therefore they are not new, but they represent without any exception the prior art, and moreover they do not need specific explanations as the man skilled in the art is perfectly able to immediately identify the construction type and the related working.

B) a blank key 2; such blank key comprises the same electronic and mechanical devices of the original key 1 , but logically, it lacks the own codes to allow the working of the same blank key, i.e. the secret code, the first Identification Code ID, and the Password; however the algorithm, identical to that one installed in the original key, and already known, is already installed into the blank key 2; furthermore logically the blank key 2 is provided with a mechanical profile, as already known, capable of permitting the introduction of the key itself into the vehicle lock, and of operating on said lock just as the original key.

C) the vehicle or central unit 3, the original key 1 is used with, and that has to use the duplicated blank key 2 too, comprises means and devices which basically perform the same function of the original key, i.e.

- a second memory capable of storing the secret code, the Password, and a second Identification Code ID,
- a second transponder containing the suitable algorithm, as already known,
- a logical or computing unit,
- further devices, in se generally known, which allow of transmitting, receiving, modulating/demodulating the radio-electric transmitted and received signals.

[0029] Moreover said central unit 3 is provided with transmission means able of transmitting an enough powerful radio-electric signal to the original key engaged to the vehicle lock, so as to start the procedure for the mutual authentication between the original key and the central unit itself.

D) a duplicating device 4, whose composition and operation are, in the principle, still similar to those of the blank key 2, and which therefore, for the sake of brevity, will not again be explained.

[0030] However it is reminded that said duplicating device is provided with the same algorithm installed into the two keys, the original key 1 and the blank key 2, and with a particularly quick and powerful computing unit, whose function will be described later on.

[0031] As for the duplicating device 4, it is generally divulgated in the PCT patent application No. published as WO 2008/145199 and there described as «reading/writing unit 13». Therefore it acquires a data that is randomly encrypted into a first encryption form.

[0032] Thus, it is provided with:

a) an internal memory and a reading knob to write the code contained into said inner memory,

b) a small antenna capable of receiving a radio-electrical signal containing a code, of transferring said code into said inner memory and, on a defined command on the writing knob, of re-transmitting outwards said code stored into it,

c) a computing unit particularly designed and produced to process at a high speed the encrypted secret code, and to identify in a very reliable way the secret code after its decryption,

E) a device capable of receiving the electro-magnetic signals coming from the central unit 3 of the vehicle, and that therefore will be called sniffer 5.

[0033] Said sniffer 5 is a device able of receiving a radio-electric signal comprising one or more codes, to store said codes without making any processing on them, and to re-transmit them, according to a pre-determined command given to it, to said duplicating device 4.

[0034] It will be also apparent that the sole function of the sniffer 5 is to intercept the signal coming from the central unit 3, to store it and to deliver it, on a command of the duplicating device 4, into the same duplicating device 4 which stores it into the suitable memories.

[0035] The method of the invention is based on the following strategy: shortly speaking, said strategy is based on the «interception» of a part of the communication between central unit and original key, on the «substitution» of the central unit itself through a proper means (the duplicating device 4 which is therefore enabled to perfectly emulate the central unit 3), on the interrogation - for the second time - of the original key in order to catch also the last part of its information, and therefore in the transferring all information to the blank key.

[0036] To sum up, going now to the operating modes, in order to implement the duplication of the blank key, the original key is as «interrogated»; such interrogation is achieved by introducing it into the vehicle lock.

[0037] (it is here omitted the step of the recognition of the ID of the original key by the central unit 3; however such step will be resumed in the complete sequence of the operating steps, which will be repeated and explained with great detail in the following).

[0038] So the central unit 3, in a known way, transmits a radio-electric interrogation signal, properly coded and encrypted by the algorithm in it installed; said interrogation encrypted signal, sent to the original key, is however received also by the sniffer 5.

[0039] The sniffer intercepts the communication between the original key and central unit, i.e.:

- the interrogation code transmitted by the central unit, and
- the secret code transmitted, as the answer, from the original key.

[0040] The sniffer 5 however stores only the encrypted code coming from the central unit 3 and neglects the encrypted code, as the answer, coming from the original key 1.

[0041] At this time the duplicating device 4, provided from the beginning with the same algorithm, is also provided with the interrogation code of the central unit 3.

[0042] This duplicating unit 4 is then enabled to implement a very complex and quite long-lasting mathematical processing, in order to exploit the algorithm installed into it to decrypt the secret code from the encrypted signal generated by the central unit 3.

[0043] Such very complex processing is based on specific mathematical functions, and is well known to the man skilled in the art, and must be implemented by proper processing means, which may be either comprised inside the duplication device 4 itself, or made-up by external means, to be connected to the duplication device 4 itself; however this type of embodiment is not included in the present invention, and therefore it will not be further detailed.

[0044] However it is possible that, from one interrogation only of the central unit, a decrypted signal which could be insufficient to identify in a reliable way the true central unit secret code; therefore an advantageous improvement of the instant method consists in the acting of the original key into its lock a number of times and successively, so as to receive from said central unit a corresponding plurality of encrypted signals which are different from each other, but which are all, if properly decrypted, to supply information in all suitable to identify the exact secret code.

[0045] It is obviously possible to carry out only one activation of the central unit 3, which therefore replies with only one coded decrypted code; however said signal could be insufficient for the duplicating device 4 to identify in an unambiguous way the secret code, and therefore it comes out to be particularly profitable to make out a sequence of activations of the central unit 3, what is practically done by making, at the beginning of the method, a series of successive rotations of the original key into its lock, which allows to give raise respective answering signals from the central unit which, properly recorded by the sniffer 5, are all flown into the duplicating device 4.

[0046] After having processed the received encrypted codes, the duplication device 4 selects the secret code from the central unit 3, and stores it into its memory.

[0047] By introducing then into the duplicating device 4 the original key 1, it, correctly interrogated by the duplication device 4 which transmits the secret code- encrypted by the algorithm now recognized by the central unit 3, replies as it received the signal of the central unit 3, as it receives the same signal; it therefore «believes» to be interrogated by the central unit, and therefore replies transmitting its own Password.

[0048] At this time the duplicating device is also informed about the Password of the original key, and therefore may store it and transfer it into the blank key, which successfully and as last operation is introduced into the duplication device 4.

[0049] To sum up, the invention strategy is based on the circumstance of «intercepting» the exchange of some information (Identification number ID, and secret code) between the original key and the vehicle central unit, of storing them and of transferring them on a proper storing means, i.e. the duplicating device 4.

[0050] It may code the central unit secret code, and then emulate the central unit working; therefore, when interrogated by the original key, receives from it the password too.

[0051] Then the duplicating device is informed of the secret data of the original key, i.e. the ID, the secret code and the PASSWORD.

[0052] Finally all these information are transferred from the duplicating device 4 into the blank key, which then acquires all information of the original key.

[0053] With reference to the Fig. 2, the actual practical method, represented in great detail through a flow-chart, is the following:

Step A) the original key is inserted into the vehicle lock, and is rotated until it closes the electric circuit which activates the central unit of the vehicle itself; profitably such rotation of the original key, and the relevant activations of the central unit 3, are more than one, and are made up in sequence.

[0054] It was also verified and evaluated that the optimum number to get a sufficient number of encrypted codes, and that may be afterwards certainly decrypted by the duplicating device 4 to get the secret code, is of three activations/rotations of the original key inside the respective lock.

[0055] It is in the fact apparent that the more the information available on a certain condition, the more are the chances of faithfully representing that condition and of avoiding identification mistakes.

Step B) The central unit transmits a radio-electric signal comprising a code of identification request of the original key, that is the first Identification Code ID, which is an «open» code;

Step B-B) The original key receives such signal requesting of said «open» ID, and transmits that code to the central unit 3;

Step B-C) The central unit receives first said open ID code and compares it to the previously stored second Identification Code ID; if it is recognized, such recognition allows the procedure continuation;

Step C) The procedure goes on; the central unit 3 sends a random encrypted code which comprises the secret code, from the algorithm, to the original key 1;

Step D) The intercepting device 5, called sniffer, arranged close to the original key, intercepts the radio-electric signal which contains both the first ID of the original key, and the interrogation of the central unit, and the key reply, i.e. its secret code in an encrypted form; however the latter is not stored, and the sniffer records and stores the central unit 3 interrogation only (the sniffer positioning close to the lock is preferably done before introducing the original key);

Step E) Said sniffer 5 is introduced into said duplicating device 4;

Step F) Said duplicating device 4 emits a radio-electric signal which reaches said sniffer 5;

Step G) Said sniffer transmits to said duplicating device 4 an electric signal with the random code encrypted by the algorithm which comprises the secret code, stored during the Step D;

Step H) The duplicating device 4 stores the random code generated by the central unit 3 and, through a plurality of mathematical functions and proper computing unit decrypts said encrypted code, so obtaining the sought code.

[0056] Now the duplicating device contains the secret code, decrypted, of the original key 1. Step I) The sniffer 5 is removed from the duplicating device 4;

Step L) Into the duplicating device 4 the original key is inserted;

Step M) The duplicating device interrogates the original key with a suitable radio-electric signal which comprises the secret code encrypted by its algorithm, so emulating the central unit operation;

Step N) The original key replies by transmitting a further own code, i.e. the encrypted password;

Step O) The duplicating device stores such Password;

Step P) The original key is removed from the duplicating device; Step Q) The blank key is introduced into the duplicating device;

Step R) The duplicating device transmits a radio-electric signal to said blank key, so transferring to it the PASSWORD, the secret code and the first ID;

Step S) The blank key stores into a definite memory all said three codes.

[0057] So the duplication of the blank key is completed. To be noted now a profitable improvement of the method, which allows a certain simplification; in the facts, if in the Step D or of interception, the sniffer 5 intercepts and stores also the secret code of the original key, the Steps M and N would be no more needed, as the secret code transmitted by the original key would have been already transmitted to the sniffer 5, and then from it to the duplicating device 4, which could immediately emulate the central unit 3 to interrogate the original key to let it transmitting to himself the respective Password.

[0058] However such methodological simplification raises the risk that, as the signal carrying the secret code of the encrypted key is very weak, due to the fact that it is emitted by the original key which is supplied by the radio-electric signal emitted by the central unit, then such signal with the encrypted secret code may be easily jammed, or anyway may be received in an incomplete or wrong, which obviously causes the interruption of the key duplication procedure.

[0059] It is to be noted moreover that some of the above described Steps are typical manual operations, that an outer operator must perform on the described means, as introduce a key and rotate it inside the lock, extract a key, activate the duplicating device, move the sniffer etc...., as the remaining steps are automatic steps which are carried out by said means in a known way.

[0060] More specifically the manual steps are Steps A, E, I, L, Q.

[0061] Steps B-C, H, O, S are steps of mere processing/comparison /storage into the respective devices, without any relationship to the other devices and therefore are only symbolically drafted.

[0062] Step D regards the intercepting action of the sniffer 5, which however shall be manually arranged and prepared close to the lock, and therefore it is intended that the sniffer positioning 5 requires an additional operation which here is not listed as a real operating Step.

[0063] By carefully observing the figure 2, it turns out to be apparent, also only by a visual check, the nature of the method strategy; as a matter of facts the original key 1 and the central 3 are put into relationship to each other (Steps A and B), so that the central unit is made to recognize and store the content of the codes stores in the original key; afterwards said codes are intercepted by the sniffer 5 (Steps C and D), which provides to transmit them to the duplicating device 4 (Steps E, F and G).

[0064] At this time the original key 1 also is introduced into the duplicating device 4 (Steps I, L), which interrogates said original key (Steps M, N) to get the answer with the password (Steps M, N).

[0065] Finally, after the Step P all coded information, originally stored in the original key 1 , are contained inside the duplicating device 4, and therefore it is now possible to introduce the blank key 2 and transfer to it all said coded information.

[0066] The just described solution, which is effective, sure, and innovative, allows then a complete duplication of a blank key from an original key which uses the technique of the "mutual authentication", without having to connect to any database placed in a remote site, accessible only with on-line means to assure the security of the code transfer.

[0067] However such method implies the presence and the working of the sniffer 5; but such constraint and need are not deprived of penalization; in the facts the presence of the sniffer 5 shows some critical aspects, as it has to work with radio- electric signals that may be miss-received and therefore may introduce errors in the transmission of information and codes; moreover the sniffer operations are delicate, and precise operations which must be carried out with great caution and with the right sequence; all that may be troublesome and unpleasant in a working environment which is little trained and sensible to the remarkable technical complexity of the involved means and methods. Such drawback often is considered not agreeable, even because it requires a cost increase and a higher complexity of the duplication procedure.

[0068] In order to avoid such problems, in the following a method is described which allows to carry out the duplication of an original key without using the sniffer.

[0069] The strategy of such improvement consists in that the blank key is used as sniffer, in the meaning that the central unit codes are introduced into the duplicating device through the blank key itself.

[0070] However to make it possible to use the blank key as "carrier" of such information, the blank key must have been previously loaded with the ID of the original key.

[0071] To this purpose, the duplicating device is employed as means to transfer the ID from the original key to the blank key; this one, after having been loaded with the ID, is used to receive from the vehicle central unit its secret code, and to store it, which then may be acquired, into the decrypted form, by the blank key itself.

[0072] It is here reminded that the secret code is the same both for the central unit 3 and for the original key 1; in the facts it could not be different, as if it were the case, it would be impossible to carry out the mutual authentication.

[0073] Therefore the blank key may transfer its still encrypted secret code into the duplicating device, which decrypts the secret code through suitable computing means and with advanced mathematical techniques.

[0074] Said computing means and said mathematical techniques are in se easily deductable from the prior art and generally are in the knowledge of the man skilled in the art, and therefore they will not be repeated.

[0075] The duplicating device now is informed of the central unit secret code, and therefore it is able of emulating it.

[0076] At this time the duplicating device is brought exactly in the same conditions where it is according to the previous procedure after the Step L, i.e. it contains both the ID and the decrypted secret code.

[0077] Therefore from this time on the procedure goes on exactly according to the Steps N, O, P, Q, R, S above described, obviously after having introduced the original key into the duplicating device.

[0078] More precisely, and with reference to Fig. 3, the flow diagram of said procedures as follows:

A-1) the original key is introduced into the duplication device 4,

B-1) the duplication device emits a first radio-electric signal which interrogates the original key,

C-1) the original key responds by emitting a second radio-electric signal which contains its ID,

D-1) Said ID is received and stored into the blank key,

E-1) The blank key is introduced into the vehicle lock and one or more attempts of starting the engine is made (the reason of carrying out more than one attempt has been already explained before),

F-1) at each attempt of starting the engine, the vehicle central unit 3 transmits to the blank key a third radio-electric signal which contains a random code encrypted by the algorithm which comprises the secret code,

G-1) The blank key is removed from the vehicle lock and introduced into the duplication device,

H-1) The duplicating device through suitable computing and mathematical functions, in se known, decrypts the secret code and stores it,

L-1) the blank key is removed from the duplicating device,

M-1) the original key is introduced into the duplicating device. From this time on, the procedure goes on as from the previous Step L, i.e.:

N-1) the duplicating device interrogates the original key with a proper fourth radio-electric signal containing the secret code, so emulating the central unit operation,

Step O-1) the original key responds by transmitting a new own code, the PASSWORD;

Step P-1) the duplicating device stores such PASSWORD,

Step Q-1) the original key is removed from the duplicating device,

Step R-1) the blank key is introduced into the duplicating device,

Step S-1) the duplicating device transmits a fifth radio-electric signal which contains: said PASSWORD, and the secret code, to said blank key; in the facts the ID has been already transmitted and stored during the previous Steps C-1 and D-1 ,

Step T-1) The blank key stores into a defined memory said PASSWORD and the secret code.

[0079] It should have been noted that the flow diagram of said Figure 3 describes the procedure only from the initial Step A-1 until the Step M-1.

[0080] As a matter of facts, the procedure goes on exactly as from the Step L of Figure 2, to which it is referred for better clarity and brevity.

[0081] Throughout this patent specification, use of the term 'algorithm' in the sense of a decryption algorithm or the like is intended to be defined by the actual steps of the algorithm as opposed to the precise computer code used to implement the algorithm. Thus, two versions of the same algorithm may be implemented with different computer code provided they define the same overall process and functionality.

CLAIMS:

1. A method for a duplication of original electronic keys, the method comprising:

intercepting a radio-electric interrogating signal of an encrypted electronic authentication system transmitted between a central processing unit of a vehicle and an original key, the radio-electric interrogating signal including therein an encrypted random code generated by an algorithm, the encrypted random code including therein a secret code, the encrypted electronic authentication system utilizing an identification code (ID), the secret code, a password, and the algorithm;

transferring said intercepted random code to a key duplicating device, the duplicating device having said algorithm installed thereon;

decrypting said secret code from said random code at said key duplicating device using said algorithm;

performing an interrogation process by transmitting a radio-electric signal, including said secret code, from said key duplicating device, to said original key;

receiving the password, transmitted by said original key, at said key duplicating device in response to the transmission of the secret code; and

transferring said password to a blank key, the blank key including the algorithm and a data storage device configured to store an identification code (ID), a secret code and a password.

2. The method according to claim 1, wherein the radio-electric interrogating signal of the encrypted electronic authentication system is transmitted from the central processing unit of the vehicle to the original key in response to a receipt of the identification code ID from the original key.

3. The method according to claim 1 or claim 2, wherein the method further comprises, before the intercepting step, a step of obtaining the identification code (ID) from the original key.

4. The method according to claim 2, wherein the method further comprises, before the intercepting step, a step of obtaining the identification code (ID) from the original key.

5. The method according to claim 3, wherein the step of obtaining the identification code (ID) from the original key further comprises:

interrogating the original key by transmitting a first radio-electric signal from said key duplicating device to the original key; and

receiving a second radio-electric signal from the original key containing an identification code (ID).

6. The method according to claim 3, wherein the step of obtaining the identification code (ID) from the original key further comprises:

intercepting a first radio-electric signal of an encrypted electronic authentication system transmitted between the original key and the central processing unit of the vehicle, the first radio-electric signal including therein the identification code (ID).

7. A method for a duplication of original electronic keys, comprising:

intercepting, via an interception device placed in proximity to an original key, at least one radio-electric signal containing an identification code (ID) and an encrypted random code and storing the intercepted identification code (ID) and the encrypted random code in a storage of the interception device, the radio-electric signal being generated by an electronic authentication system of a vehicle performing authentication by

transmitting, by a processing unit and in response to an activation of a central processing unit, the radio-electric signal including an identification request for the identification code (ID) of the original key, to the original key,

transmitting, from the original key, the identification code (ID) stored in the original key to the central processing unit,

comparing, at the central processing unit, the identification code (ID) with a previously stored corresponding ID code, and

in response to a positive result from the comparing, generating, at the central processing unit, a random code encrypted by an algorithm, which includes a secret code, and sending the random code to the original key;

transmitting, from an interception device to a duplicator device having said algorithm installed thereon, the intercepted identification code (ID) and the encrypted random code; and

decrypting, at the duplicator device and using said algorithm, said encrypted secret code from the encrypted random code.

8. The method of claim 7, further comprising the step of before the intercepting step, introducing the original key into a vehicle lock of the vehicle and rotating the original key, the rotation of the original key closing an electric circuit activating the central processing unit of the vehicle.

9. The method of claim 7 or claim 8, further comprising:

inserting the original key into the duplicator device;

interrogating the original key by transmitting a radio-electric signal which contains the secret code encrypted by the algorithm, thereby emulating functioning of the processing unit;

receiving, from the original key, a password in response to the transmission of the secret code;

storing the password received from the original key;

removing the original key from the duplicator device;

inserting a blank key into the duplicator device;

transmitting a radio-electric signal to said blank key containing the password, the secret code and the identification code ID; and

storing, in the blank key, the password, the secret code and the identification code ID within a defined memory.

10. A method for a duplication of original electronic keys, comprising:

a) interrogating an original key by transmitting a radio-electric signal from a key duplicating device to the original key inserted into the key duplicating device, the original key and key duplicating device including a common decrypting algorithm;

b) receiving a radio-electric signal from the original key containing an identification code (ID);

c) storing said identification code ID into a blank key;

d) receiving, at the blank key, in response to an attempt at ignition from the blank key inserted into a vehicle lock of a vehicle, and from a central processing unit of the vehicle, a radio-electric signal containing an encrypted secret code;

e) decrypting, at the key duplicating device, the secret code using said algorithm;

f) interrogating, at the key duplicating device, the original key with a radio-electric signal containing the secret code in order to emulate vehicle operation;

g) receiving, at the key duplicating device, a passcode from the original key in response to the interrogating;

h) transmitting, from the key duplicating device to the blank key, the passcode and the secret code; and

i) storing, into a defined memory of the blank key, the passcode and the secret code.

11. The method according to claim 10, wherein the method further comprises the steps of, before step e) and after step d),

removing the blank key from the vehicle lock; and

introducing the blank key into the key duplicating device.

12. The method according to claim 10 or claim 11, wherein the method further comprises the steps of, before step f) and after step e),

removing the blank key from the key duplicating device; and

introducing the original key into the key duplicating device.

13. The method according to any one of claims 10 to 12, wherein the method further comprises the steps of, before step h) and after step g),

storing the passcode in the key duplicating device;

removing the original key from the key duplicating device; and

introducing the blank key into the key duplicating device.

14. The method according to any one of claims 10 to 13, wherein the method further comprises the steps of, before step d) and after step c),

inserting the blank key into the vehicle lock of the vehicle; and

attempting ignition of the vehicle using the blank key one or more times.

15. The method according to claim 14, wherein the step of attempting ignition of the vehicle further comprises: attempting ignition of the vehicle using the blank key three times.

16. A method of duplicating a motor vehicle electronic key, comprising:

transmitting to the motor vehicle electronic key, by a first device, an encrypted secret code;

receiving, by the motor vehicle electronic key, the encrypted secret code;

as the electronic key is receiving the secret code which has been encrypted, intercepting the transmission to the motor vehicle electronic key by the first device, comprising the encrypted secret code, and storing, by a second device different from the first device and different from the motor vehicle electronic key, the encrypted secret code, which is extracted from the transmission;

interrogating the motor vehicle electronic key, by a duplicator device which is different from the first device and different from the motor vehicle electronic key, using the encrypted secret code which has been intercepted and stored;

receiving, by the duplicator device from the motor vehicle electronic key, a password transmitted from the motor vehicle electronic key in response to the interrogating;

storing, by the duplicator device, the password transmitted from the motor vehicle electronic key;

transmitting, by the duplicator device, the password to a blank key; and

storing the password in the blank key.

17. The method according to claim 16, further comprising:

sending, by a first device, an interrogating signal to the motor vehicle electronic key requesting identification information; and

transmitting by the motor vehicle electronic key to the first device, an identification of the motor vehicle electronic key, in response to the interrogating signal,

wherein the transmitting by the first device of the encrypted secret code to the motor vehicle electronic key is performed in response to the transmitting by the motor vehicle electronic key the identification of the motor vehicle electronic key.

18. The method according to claim 17, further comprising:

decrypting, by the duplicator device, the encrypted secret code to form a decrypted secret code;

encrypting, by the duplicator device, the decrypted secret code to form the encrypted secret code,

wherein the interrogating of the motor vehicle electronic key is performed by using the encrypted secret code by the duplicator device.

19. The method according to claim 17 or claim 18, further comprising:

transmitting, by the duplicator device, the identification of the motor vehicle electronic key; and

storing, in the blank key, the identification of the motor vehicle electronic key.

20. The method according to any one of claims 17 to 19, further comprising:

transmitting, by the duplicator device, the encrypted secret code; and

storing, in the blank key, the encrypted secret code.

21. The method according to any one of claims 16 to 20, wherein:

the intercepting is performed by the second device which is a sniffer device which is different from the first device and the duplicator device; and

the method further comprising transmitting the encrypted secret code obtained during the intercepting by the sniffer device to the duplicator device.

22. A system for duplicating a motor vehicle electronic key which operates when there is a transmission to the motor vehicle electronic key, by a first device, an encrypted secret code and when there is a receiving, by the motor vehicle electronic key, the encrypted secret code, the system comprising:

a receiver which, as the motor vehicle electronic key is receiving the encrypted secret code, intercepts the transmission to the motor vehicle electronic key by the first device, comprising the encrypted secret code, and stores the encrypted secret code, which is extracted from transmission;

a transmitter, which is part of a duplicator device and different from the first device, which interrogates the motor vehicle electronic key using the encrypted secret code which has been intercepted and stored;

a receiver, which is part of the duplicator device, which receives from the motor vehicle electronic key, a password transmitted from the motor vehicle electronic key in response to the interrogating;

a memory, within the duplicator device, which stores the password transmitted from the motor vehicle electronic key;

a transmitter, which is part of the duplicator device, which transmits the password to a blank key.

23. The system according to claim 22, further comprising:

a decryptor which decrypts, within the duplicator device, the encrypted secret code to form a decrypted secret code;

an encryptor which encrypts, within the duplicator device, the decrypted secret code to form the encrypted secret code,

wherein the transmitter which interrogates the motor vehicle electronic key uses the encrypted secret code by the duplicator device.

24. The system according to claim 22 or claim 23, wherein the duplicator device comprises:

a transmitter which transmits an identification of the motor vehicle electronic key to the blank key.

25. The system according to claim 24, wherein the duplicator device comprises:

a transmitter which transmits the secret code to the blank key.

26. The system according to any one of claims 22 to 25, further comprising:

a sniffer, different from the duplicator device, which includes the receiver which intercepts and stores the encrypted secret code.

27. Method for a duplication of original (1) electronic keys provided with coded and encrypted electronic authentication means, comprising:

intercepting by an intercepting device (5) a radio-electric interrogating signal transmitted between a central processing unit (3) of a vehicle and an original key (1), said radio-electric interrogating signal including therein an encrypted random code encrypted by an algorithm installed into said central processing unit (3), said encrypted random code including therein a secret code, said coded and encrypted electronic authentication means comprising an identification code (ID), said secret code, a password and said algorithm;

storing said encrypted random code by said interceptive device (5);

transferring said encrypted random code from said interception device (5) to a key duplicating device (4) provided with said algorithm;

decrypting said secret code from said encrypted random code at said key duplicating device (4) by exploiting said algorithm;

interrogating said original key (1) by transmitting a radio-electric signal, including said secret code decrypted by said key duplicating device (4), from said key duplicating device (4) to said original key;

receiving said password transmitted by said original key (1) to said key duplicating device (4) in response to the transmission of said secret code; and

transferring said secret code and said password from said key duplicating device (4) to a blank key (2), said blank key (2) being provided with data storage means able of storing said identification code (ID), said secret code and said password.

28. The method according to claim 27, wherein said radio-electric signal is transmitted from said central processing unit (3) to said original key (1) in response to a receipt of said identification code (ID) from said original key (1).

29. The method according to claim 27, wherein it further comprises, before said intercepting step, a step of obtaining said identification code (ID) from said original key (1).

30. The method according to claim 29, wherein said step of obtaining said identification code (ID) from the original key (1) comprises:

introducing said original key (1) into a vehicle lock and rotating said original key (1) until closing an electric circuit activating said central processing unit (3);

transmitting a radio-electric signal from said central processing unit (3) to said original key (1), said radio-electric signal requesting said identification code (ID) of said original key (1);

transmitting said identification code (ID) from said original key (1) to said central processing unit (3) in response to a receipt of said radio-electric signal, said central processing unit (3) comparing said identification code (ID) of said original key (1) with an ID code previously stored into said central processing unit (3);

intercepting by said intercepting device (5) said identification code (ID) transmitted by said original key (1) and transferring said identification code (ID) from said intercepting device (5) to said key duplicating device (4).

31. The method according to any one of claims 27 to 30, wherein said intercepting device (5) is placed close to said original key (1).

32. Method for a duplication of original electronic keys (1) provided with coded and encrypted electronic authentication means including and identification code (ID), a secret code and a password, comprising:

inserting an original key (1) into a key duplicating device (4) and interrogating said original key (1) by transmitting a first radio-electric signal from said key duplicating device (4) to said original key (1);

transmitting a second radio-electric signal from said original key (1) in response to said first radio-electric signal, said second radio-electric signal containing said identification code (ID) of said original key (1);

receiving and storing said identification code (ID) into a blank key (2);

introducing said blank key (2) into a vehicle lock and attempting at vehicle ignition one or more times;

in response to said attempting at vehicle ignition, transmitting a third radio-electric signal from a central processing unit (3) of said vehicle to said blank key (2), said third radio-electric signal including therein an encrypted random code encrypted by an algorithm installed into said central processing unit (3), said encrypted random code including therein said secret code;

removing said blank key (2) from said vehicle lock and introducing said blank key (2) into said key duplicating device (4);

decrypting said secret code at said key duplicating device (4) through computing and mathematical functions;

removing said blank key (2) from said key duplicating device (4) and interrogating said original key (1) at said key duplicating device (4) with a fourth radio-electric signal containing said secret code, decrypted by said key duplicating device (4), in order to emulate said central processing unit (3);

receiving and storing at said key duplicating device (4) said password of said original key (1) transmitted in response to said interrogation;

introducing said blank key (2) into said key duplicating device (4) and transmitting from said key duplicating device (4) to said blank key (2) a fifth radio-electric signal containing said secret code and said password; and

storing into a defined memory of said blank key (2) said secret code and said password.

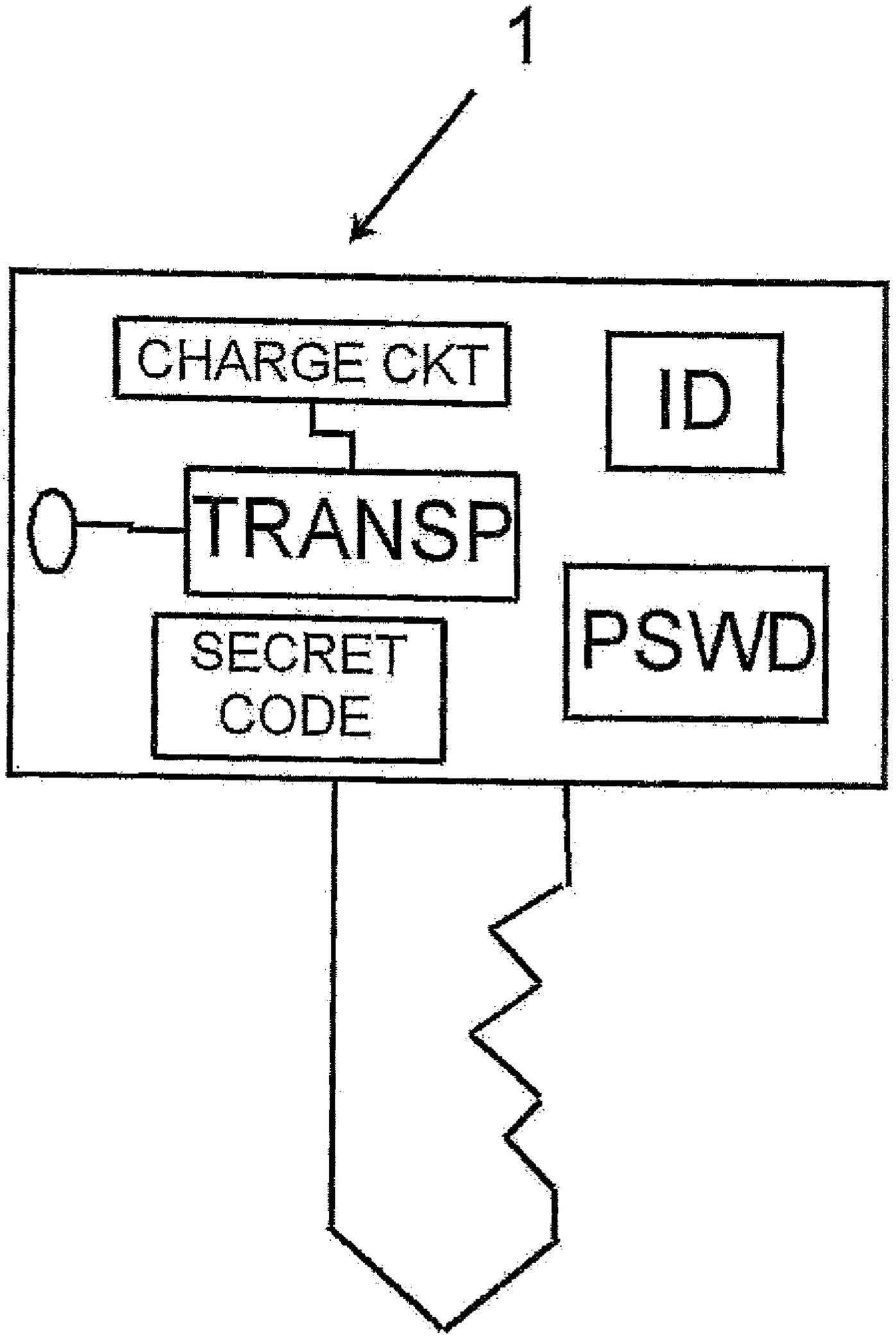


FIG. 1A

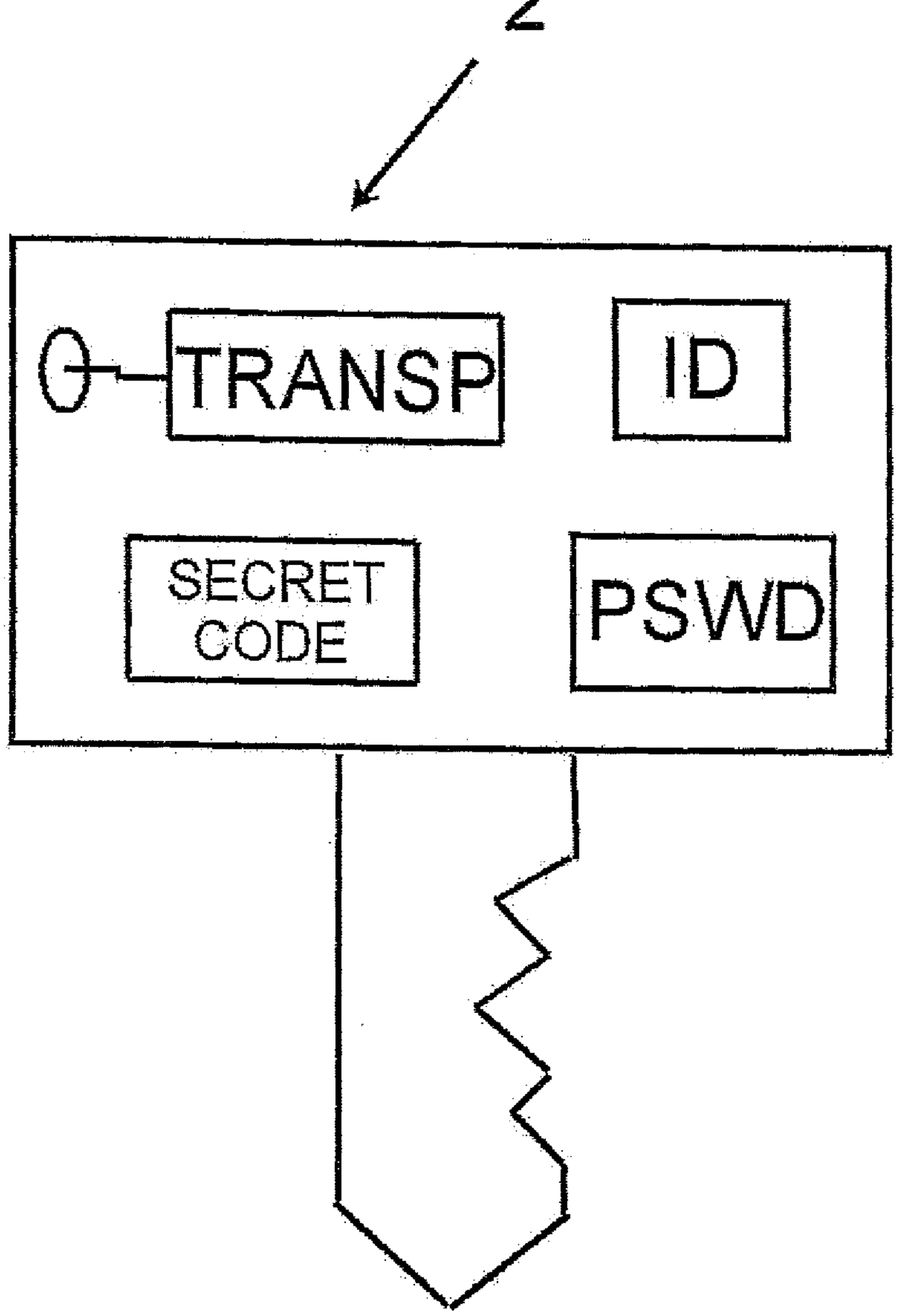


FIG. 1B

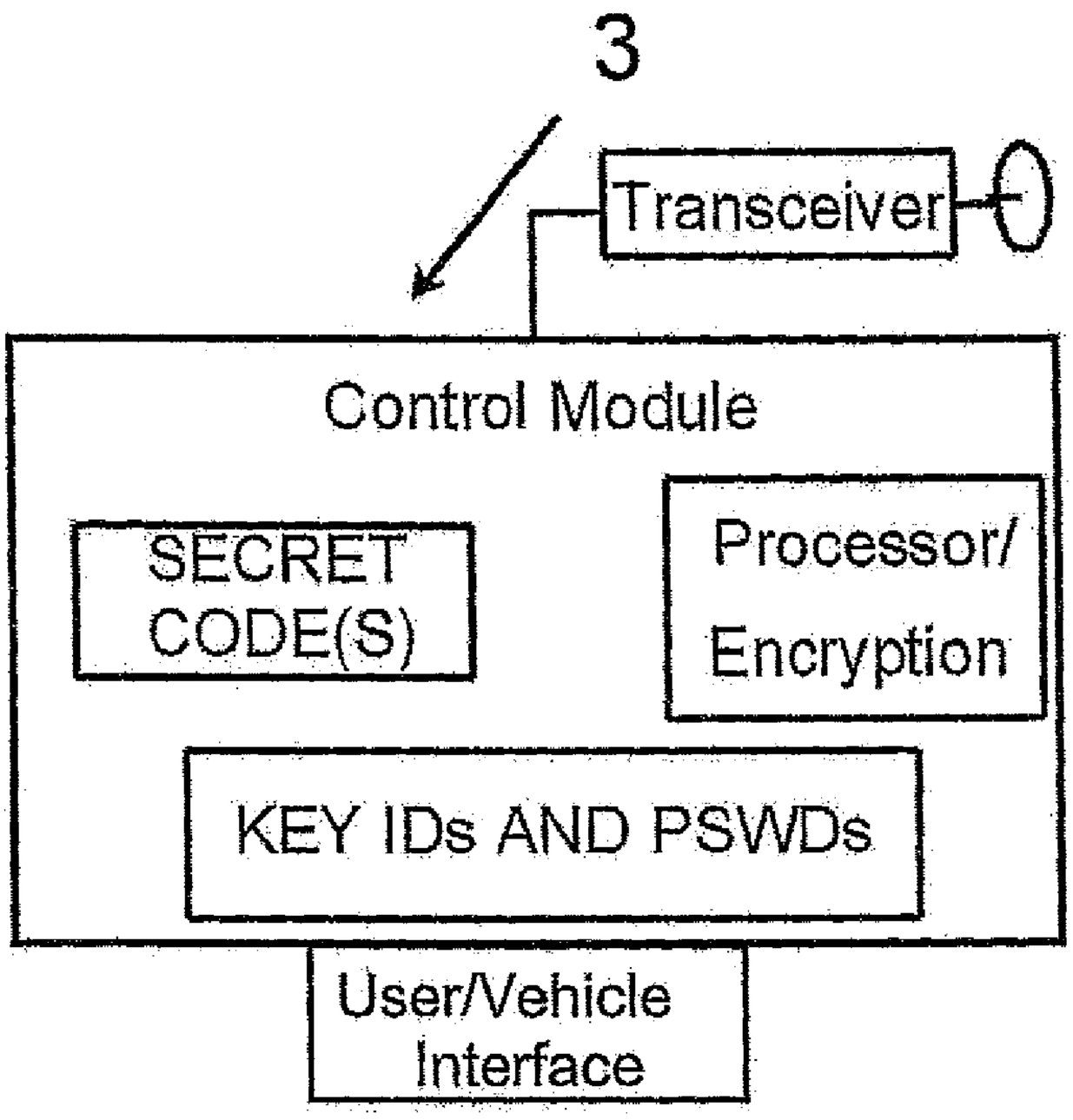

3
Transceiver
Control Module
SECRET CODE(S)
Processor/ Encryption
KEY IDs AND PSWDs
User/Vehicle Interface

FIG. 1C

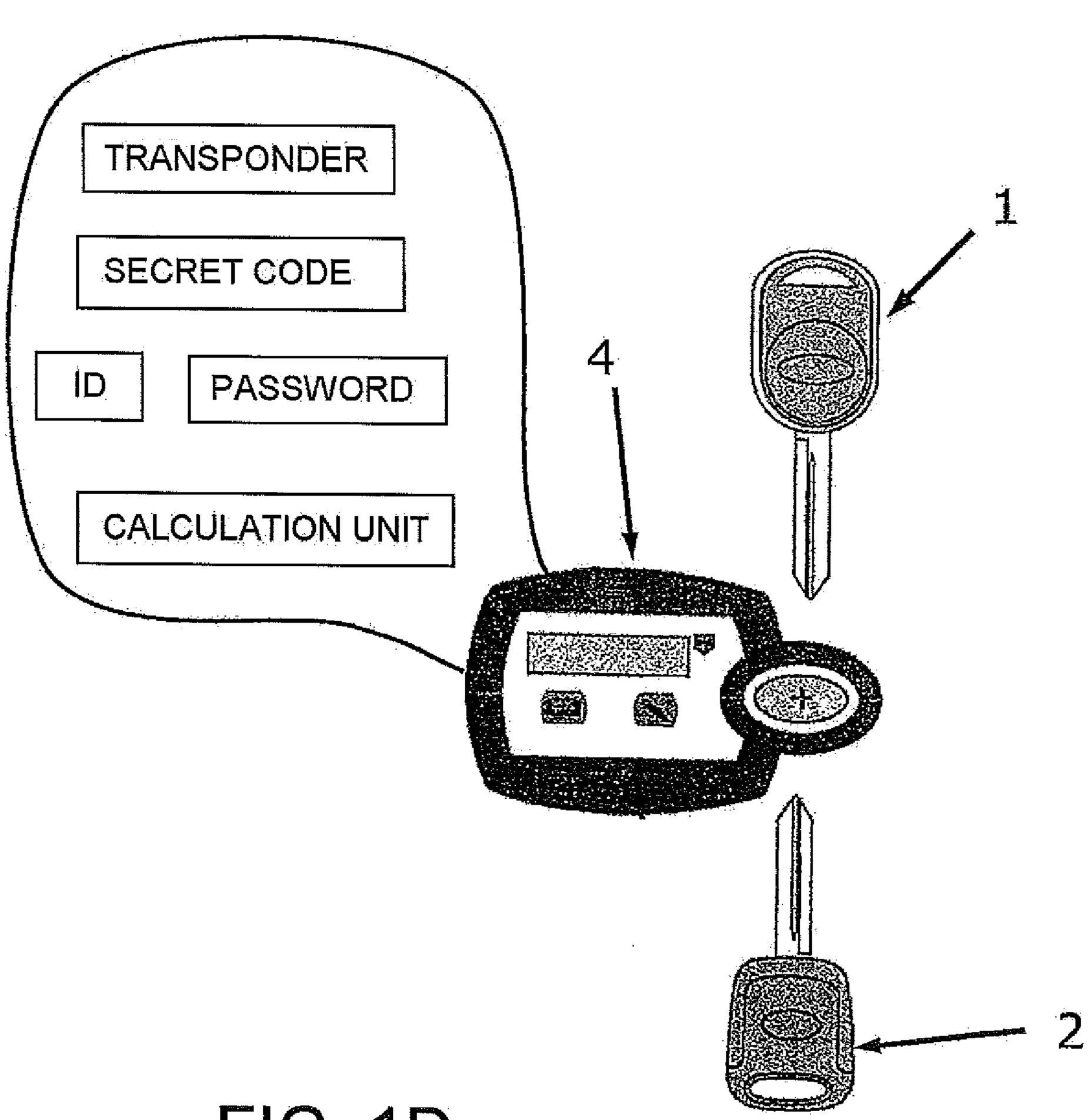


FIG. 1D

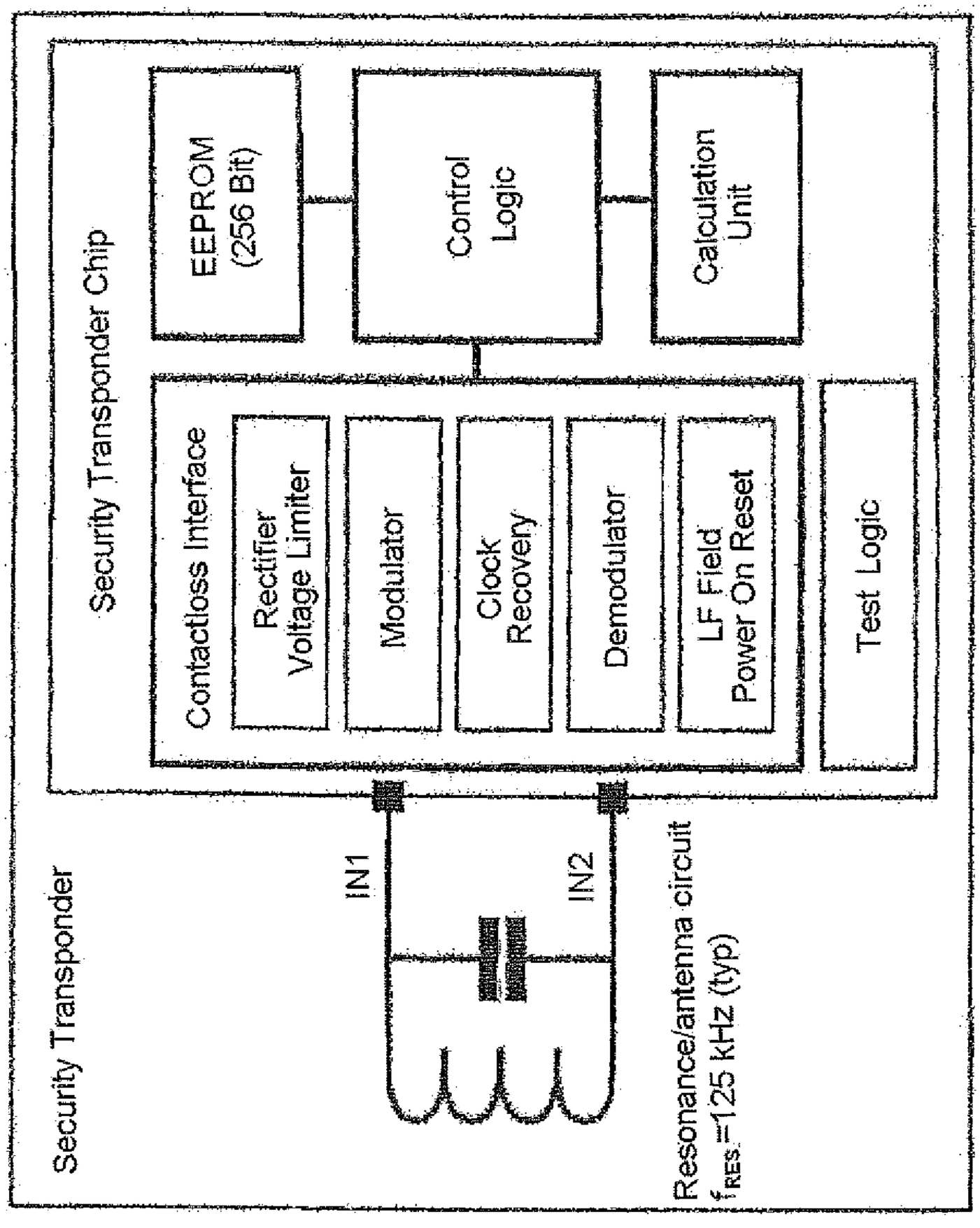

Security Transponder Chip
EEPROM (256 Bit)
Control Logic
Calculation Unit
Contactloss Interface
Rectifier Voltage Limiter
Modulator
Clock Recovery
Demodulator
LF Field Power On Reset
Test Logic
Security Transponder
IN1
IN2
Resonance/antenna circuit
$f_{RES.}$=125 kHz (typ)

FIG 3

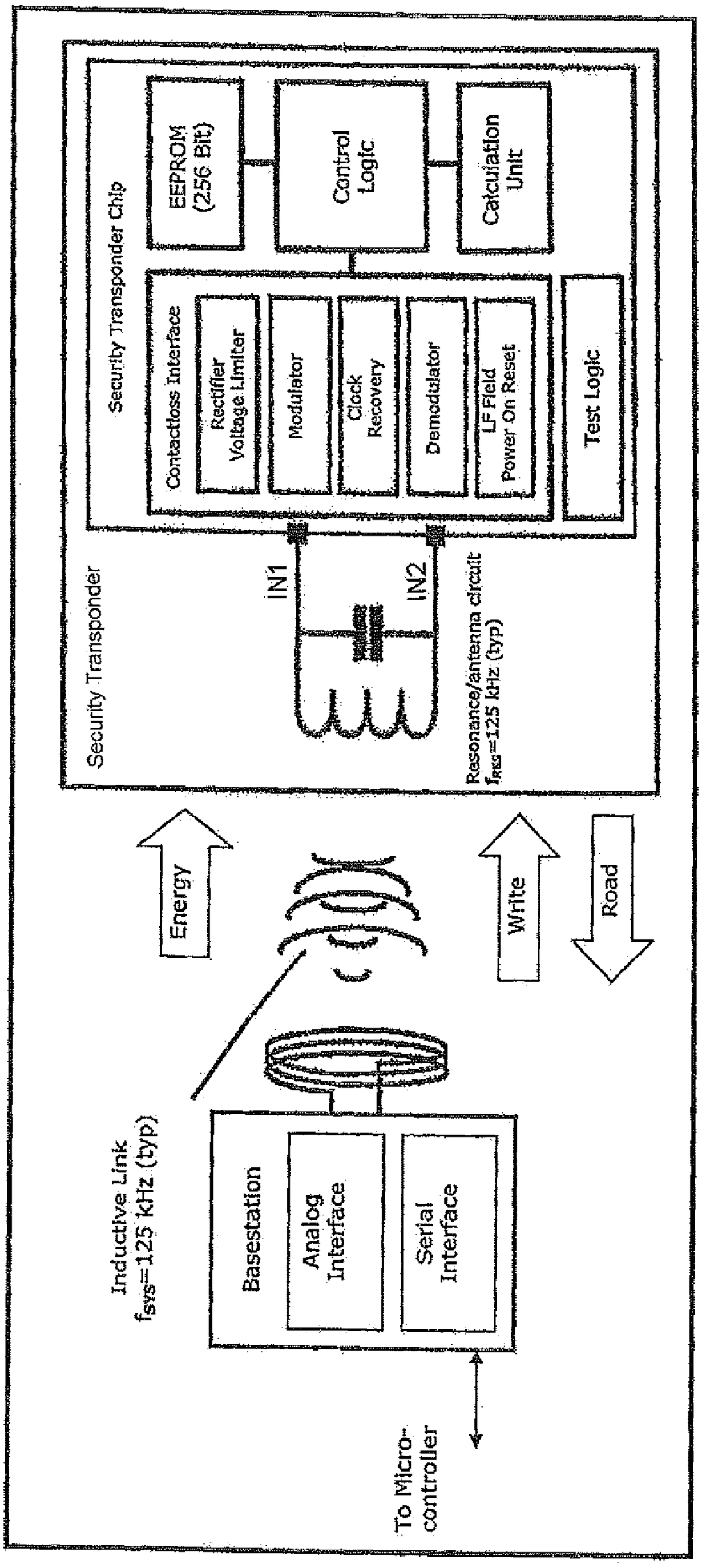

Security Transponder Chip
EEPROM (256 Bit)
Control Logic
Calculation Unit
Security Transponder
Contactless Interface
Rectifier Voltage Limiter
Modulator
Clock Recovery
Demodulator
LF Field Power On Reset
Test Logic
IN1
IN2
Resonance/antenna circuit
fRES=125 kHz (typ)
Energy
Write
Road
Inductive Link
fsys=125 kHz (typ)
Basestation
Analog Interface
Serial Interface
To Micro-controller

FIG. 1F

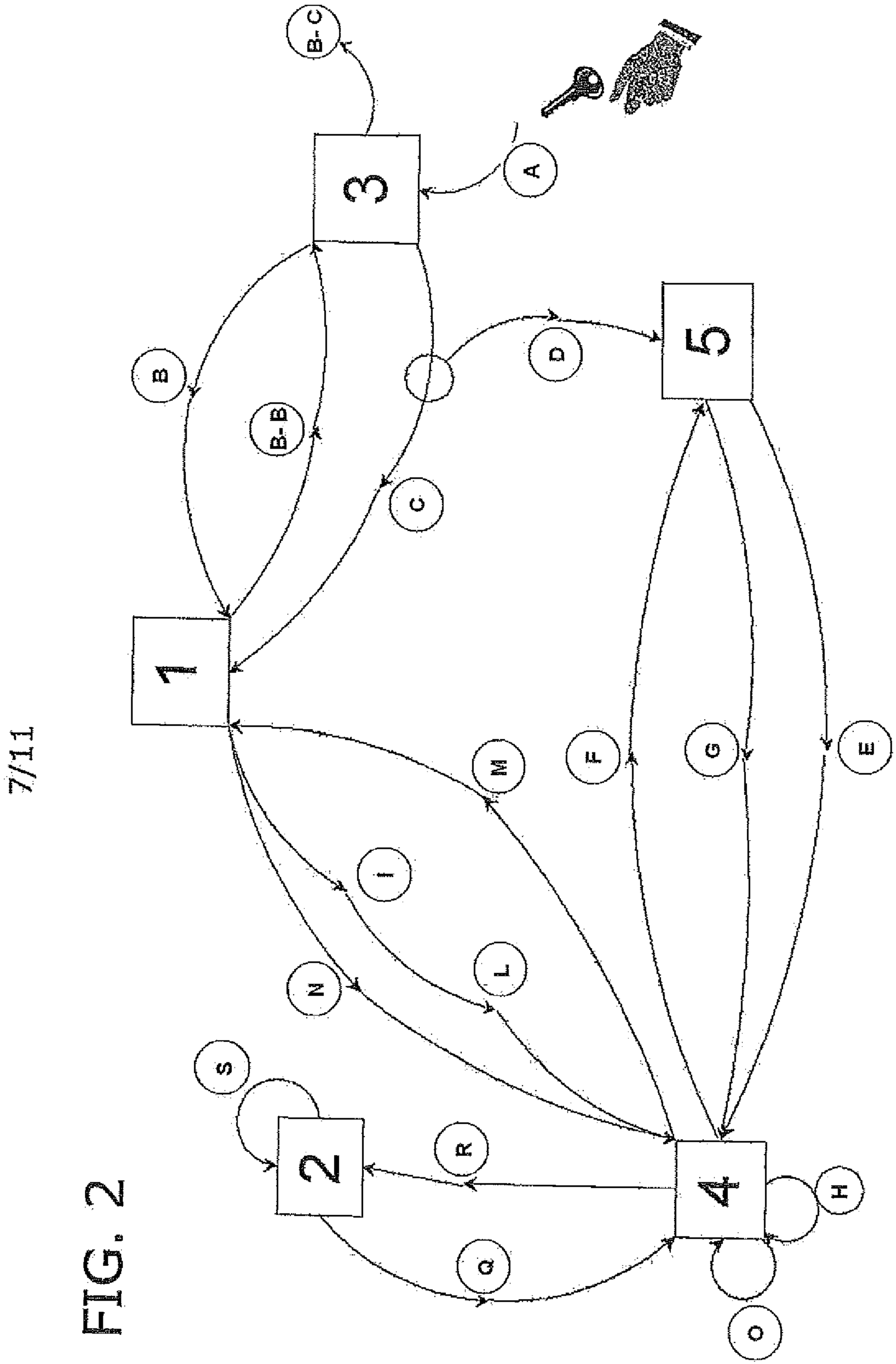


FIG. 2

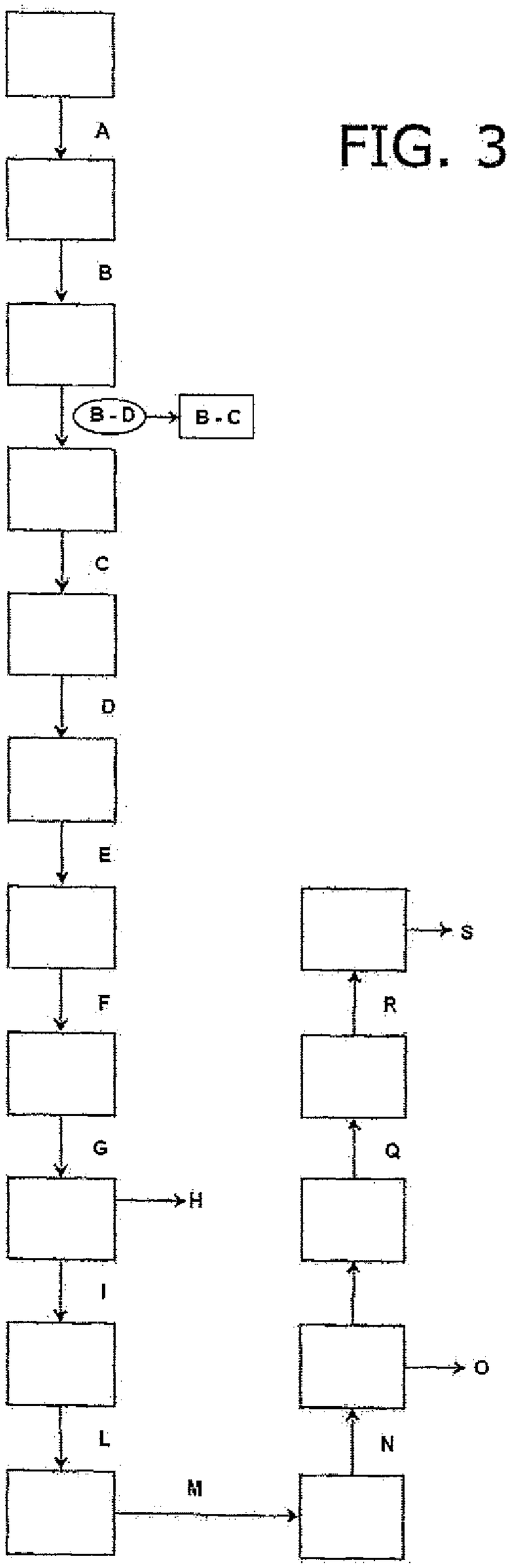


FIG. 3

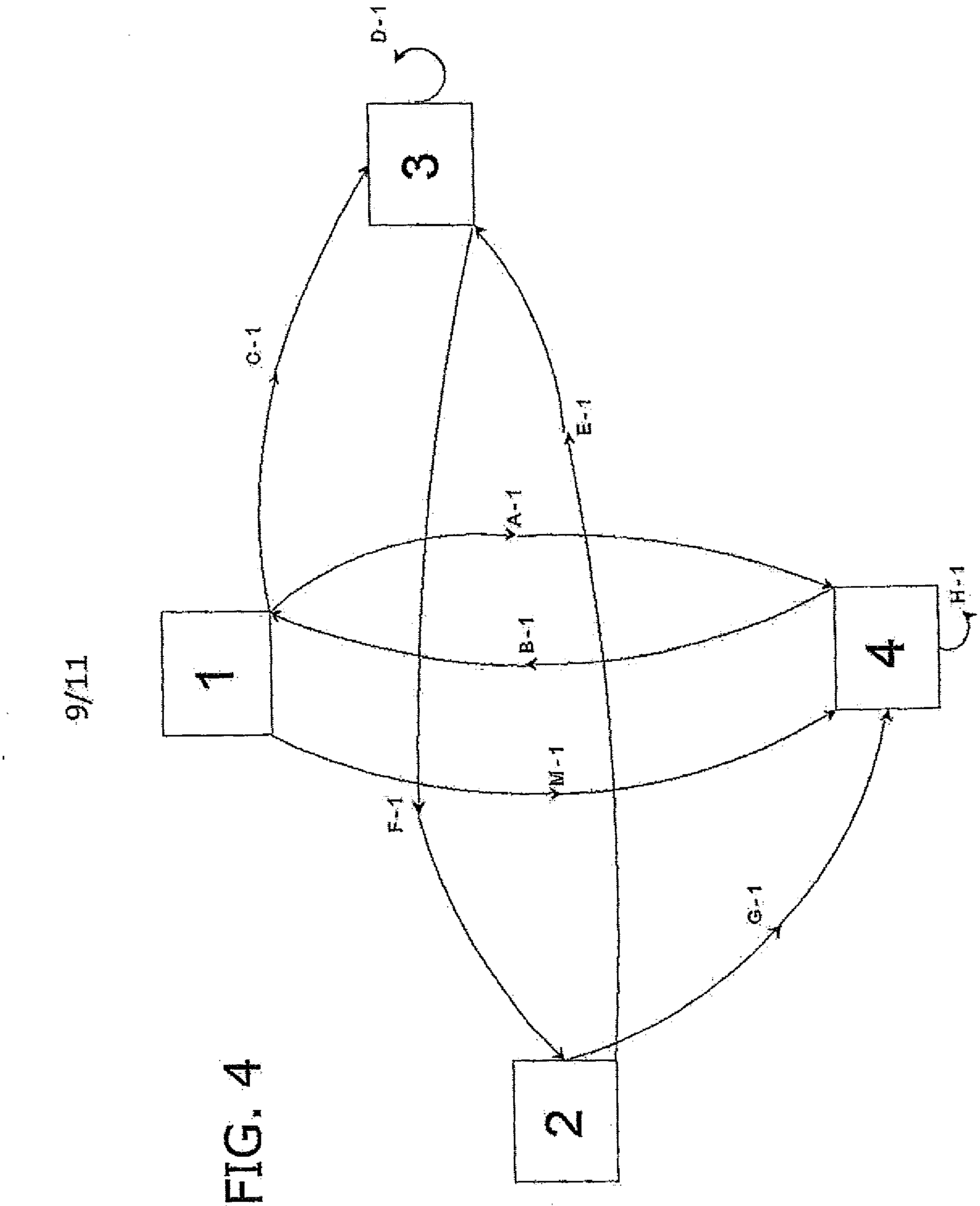


FIG. 4

FIG. 5

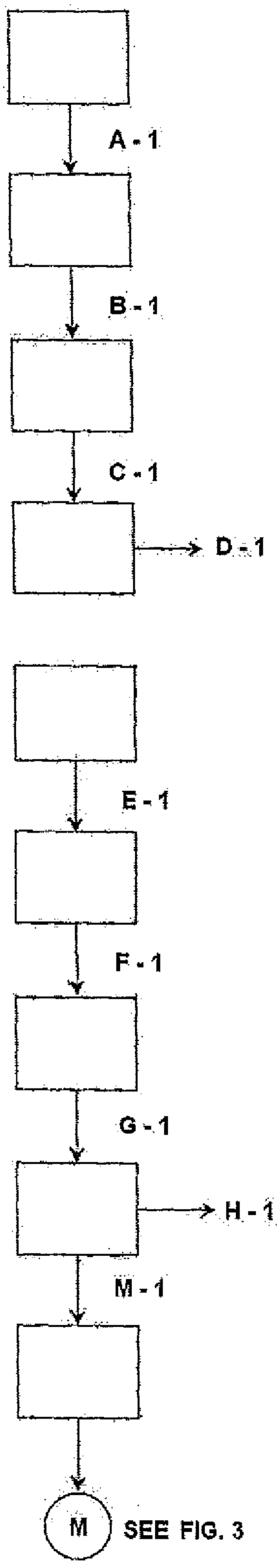
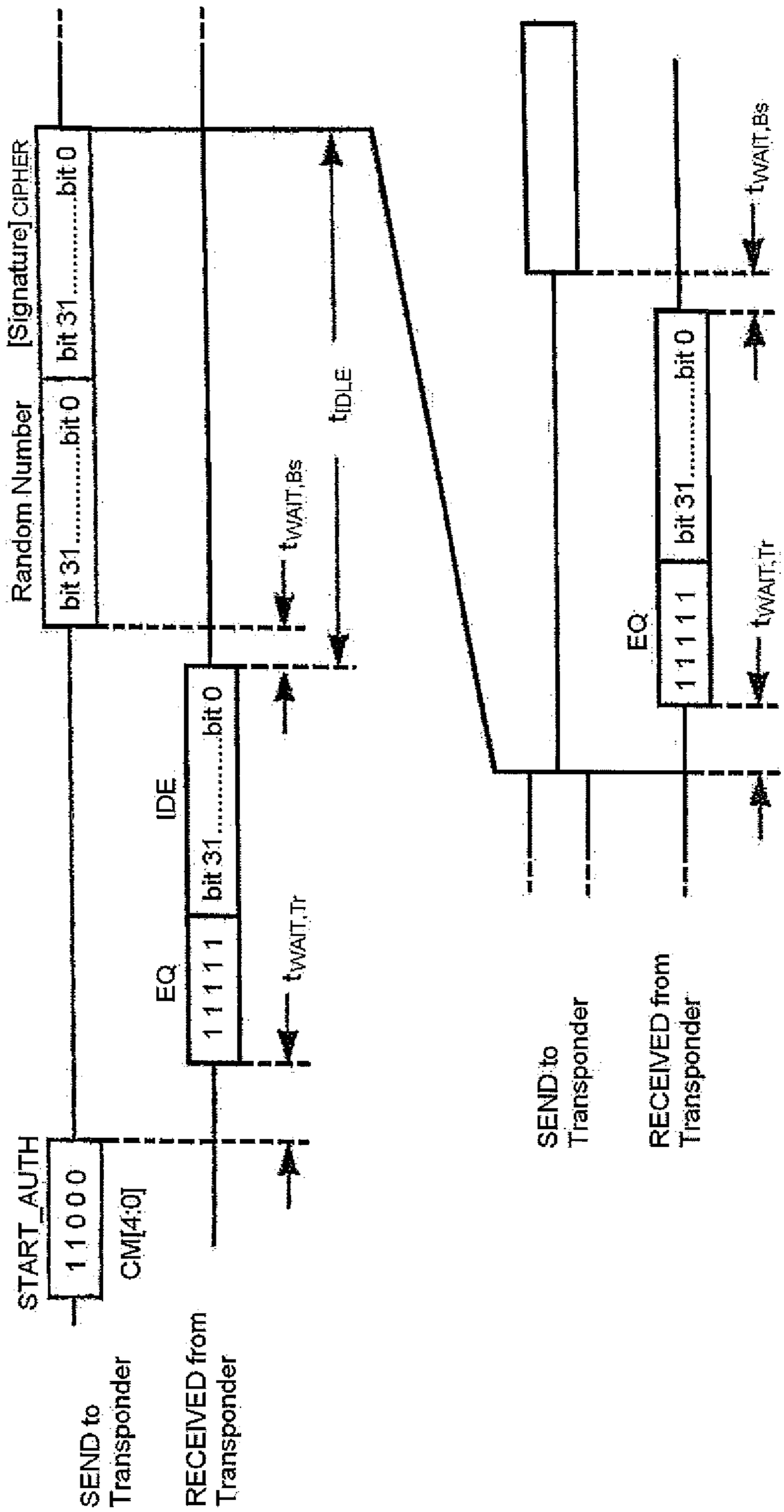
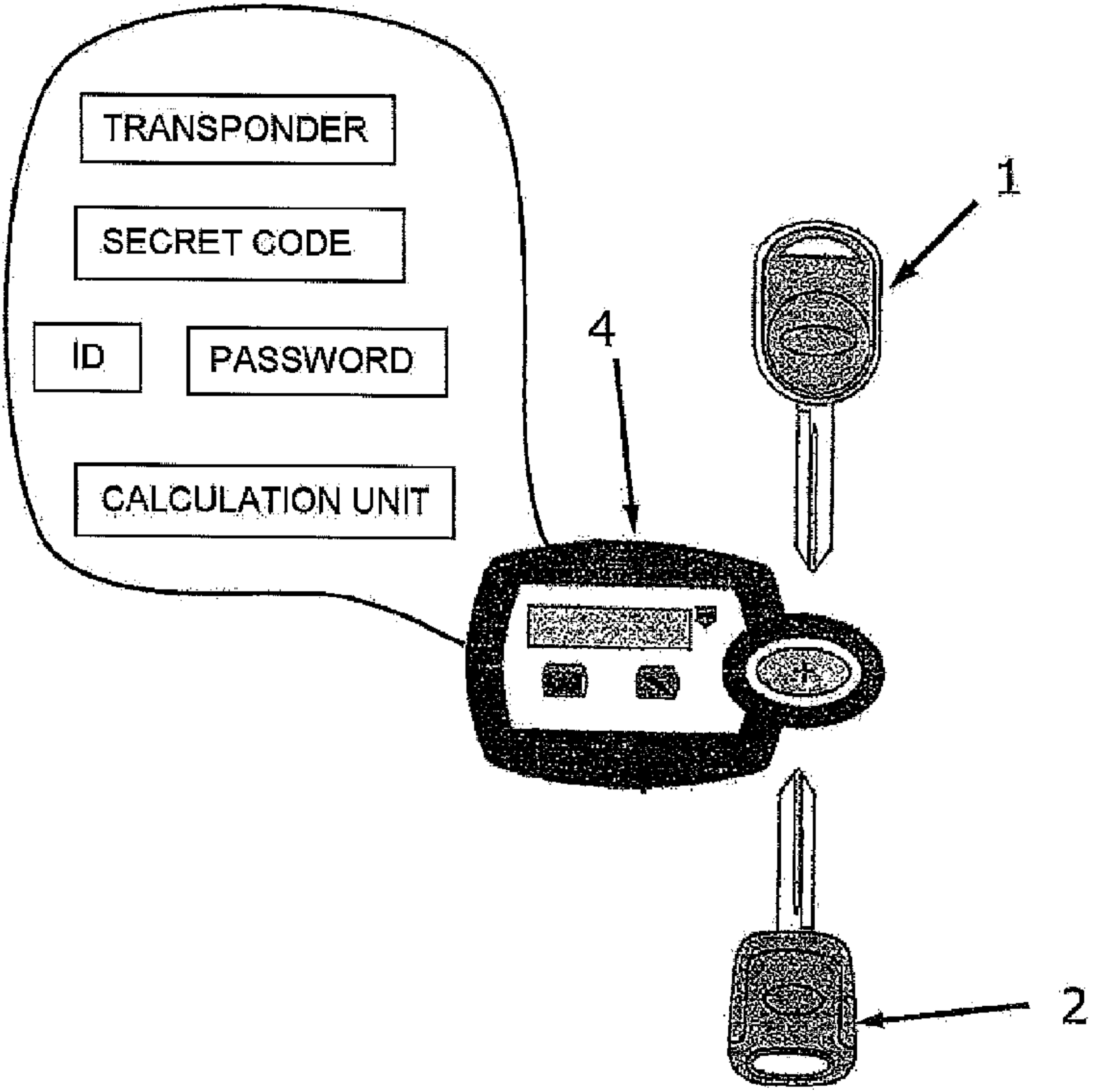


FIG. 6


SEND to Transponder
RECEIVED from Transponder
START_AUTH
11000
CM[4:0]
IDE
EQ
11111
bit 31.....bit 0
$t_{WAIT,Tr}$
$t_{WAIT,Bs}$
t_{IDLE}
Random Number
[Signature]CIPHER


TRANSPONDER
SECRET CODE
ID
PASSWORD
CALCULATION UNIT
1
4
2