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

(11) EP 1 152 108 A2

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
07.11.2001 Bulletin 2001/45

(51) Int Cl.[7]: **E05B 49/00**, B60R 25/00

(21) Numéro de dépôt: **01401095.3**

(22) Date de dépôt: **27.04.2001**

(84) Etats contractants désignés:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Etats d'extension désignés:
AL LT LV MK RO SI

(30) Priorité: **03.05.2000 FR 0005626**

(71) Demandeur: **Delphi Technologies, Inc.**
Troy, MI 48007 (US)

(72) Inventeur: **Lelandais, Guy**
91190 Gif-Sur-Yvette (FR)

(74) Mandataire: **Abello, Michel**
Cabinet Peuscet,
78, avenue Raymond Poincaré
75116 Paris (FR)

(54) Système d'accès dit mains libres pour véhicule automobile

(57) Système d'accès dit mains libres pour véhicule automobile (V), comportant un dispositif d'identification (I) apte à établir une communication bidirectionnelle avec une unité centrale de commande embarquée sur le véhicule, ladite unité centrale étant apte à engendrer, lors de la communication, un train de bits d'anti-piratage, chaque bit dudit train étant émis vers le dispositif d'identification sous la forme d'un signal radio-fréquence représentatif dudit bit, de façon que lorsque le dispositif d'identification reçoit ledit signal, ce dernier est réémis par le dispositif d'identification avec un temps de retard supérieur au temps d'émission utile du bit, et que la réception par l'unité centrale de commande dudit signal réémis déclenche l'émission par l'unité centrale du signal représentatif du bit suivant dans ledit train, le nombre de bits émis ou reçus dudit train, étant compté par un compteur 68 de l'unité centrale, de façon que celle-ci compare ledit nombre et la durée réelle correspondant à l'émission ou à la réception dudit nombre de bits, afin de déterminer, au-delà d'une valeur de seuil prédéterminée, une tentative de piratage provoquant l'arrêt de ladite communication.

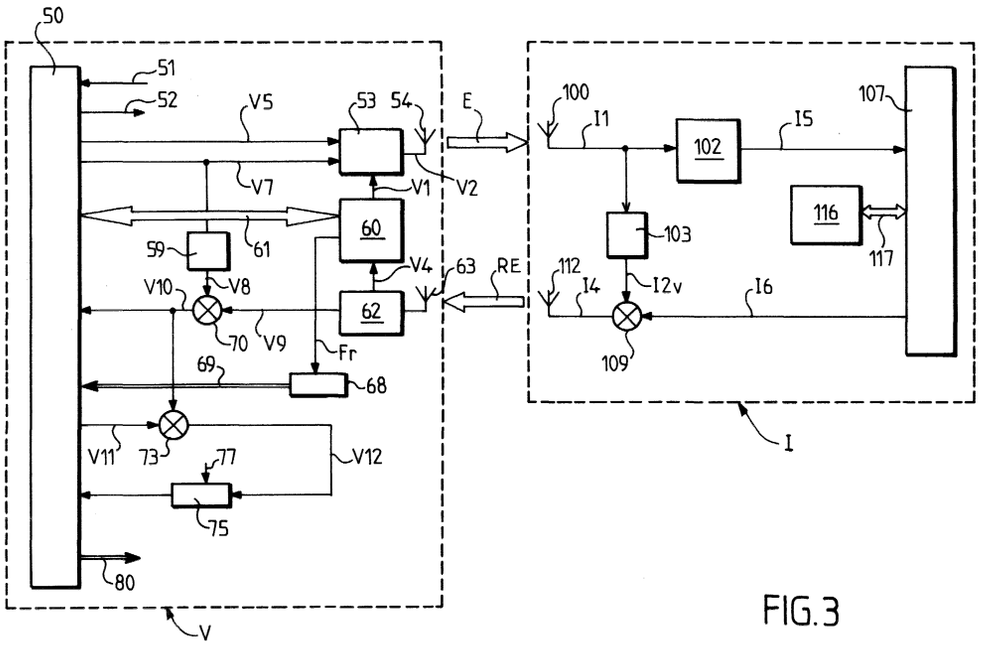

FIG.3

EP 1 152 108 A2

Description

[0001] La présente invention concerne un système d'accès dit mains libres pour véhicule automobile, c'est à dire un système de communication non filaire permettant d'entrer dans le véhicule sans clé. Ce système peut également s'appliquer au démarrage mains libres du véhicule, c'est à dire au démarrage sans clé.

[0002] Un tel système comporte généralement un dispositif d'identification destiné à être porté par un utilisateur et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique. L'initialisation du protocole de communication peut être activée en actionnant la poignée extérieure de porte, pour l'accès mains libres, ou en appuyant sur un bouton de démarrage, dans le mode démarrage mains libres. Le système est apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, généralement de l'ordre de quelques mètres, pour éviter, d'une part, les interférences avec d'autres sources de signaux de l'environnement, et, d'autre part, pour éviter le fonctionnement du système à une distance telle que l'utilisateur est trop éloigné du véhicule pour être conscient des opérations effectuées par ledit système.

[0003] Certains systèmes actuellement proposés utilisent des systèmes à induction magnétique à très courte portée, pour à la fois alimenter en énergie et transporter les informations depuis l'unité centrale du véhicule vers le dispositif d'identification qui se trouve dans le champ électromagnétique engendré par les antennes du véhicule. Toutefois, un tel système ne permet une communication qu'à très courte distance du véhicule de l'ordre de quelques cm. Un autre système couramment proposé consiste à utiliser des ondes porteuses à basse fréquence, de l'ordre de 125 kHz pour la communication depuis le véhicule vers le dispositif d'identification, et des ondes porteuses à ultra haute fréquence, par exemple de l'ordre de 434 ou 868 MHz, pour la zone Europe, et de 315 ou 902 MHz pour la zone USA. Toutefois, dans ce cas, le dispositif d'identification doit comporter une pile pour alimenter ses circuits électroniques propres. Pour minimiser la consommation électrique, on peut prévoir, à titre d'exemple, que le dispositif d'identification soit en sommeil pendant 9 ms et en éveil 1 ms, pendant des périodes de 10 ms.

[0004] Bien entendu, la communication bidirectionnelle entre le véhicule et le dispositif d'identification est cryptée, afin d'éviter tout fonctionnement intempestif du système et pour le sécuriser vis à vis des malfaiteurs. Sur la figure 1 des dessins annexés, on a représenté un exemple de système d'encryptage déjà connu. Sur cette figure 1, on a représenté un véhicule V qui comporte dans son unité centrale une mémoire 1 contenant une clé secrète K et un générateur de nombres aléatoires 2, les nombres aléatoires R engendrés ayant, par exemple, une longueur de 56 bits. Ce nombre aléatoire R est émis vers le dispositif d'identification I, comme indiqué par la flèche 3. Simultanément, ce même nombre aléatoire R est mélangé avec la clé secrète K suivant une fonction associative complexe f, dans un mélangeur 4 qui est relié à son entrée à la mémoire 1 et au générateur de nombres aléatoires 2. Le mélangeur 4 délivre, en sortie, un signal représentatif du mélange de la clé secrète K et du nombre aléatoire R, à savoir le signal f(R, K). Ce signal est mémorisé dans une mémoire 5 reliée à la sortie du mélangeur 4. Ce signal est envoyé au dispositif d'identification I, sous la forme d'un signal d'une longueur par exemple de 28 bits, comme indiqué par la flèche 6. Dans le véhicule V, le signal f(R, K) est mélangé à nouveau à la clé secrète K dans un mélangeur 7, qui est relié à son entrée aux mémoires 1 et 5 précitées. Ce mélangeur 7 mélange les deux signaux suivant une fonction associative complexe g. Le véhicule V mémorise alors dans une mémoire 8 reliée à la sortie du mélangeur 7 le signal représentatif du mélange, à savoir le signal g(R, f, K).

[0005] Du côté du dispositif d'identification, la même clé secrète K est mémorisée dans une mémoire 11 et un mélangeur 14 ayant la même fonction associative f reçoit en entrée la clé secrète fournie par la mémoire 11 du dispositif d'identification I et le nombre aléatoire R reçu par le dispositif d'identification en provenance du véhicule. Le dispositif d'identification I mémorise le signal en sortie du mélangeur 14 dans une mémoire 15 et compare ce signal dans un comparateur 16 avec le signal reçu suivant la flèche 6 en provenance du véhicule V. Si les deux signaux ne sont pas identiques, sous réserve du temps de retard propre au matériel et à la transmission du signal dans la zone de transmission autorisée, le dispositif d'identification interrompt la communication comme étant non-autorisée. En revanche, si les deux signaux correspondent, le signal est mélangé dans un mélangeur 17 avec la clé secrète fournie par la mémoire 11 du dispositif d'identification I, suivant la même fonction associative g précitée. Le signal de sortie du mélangeur 17 est mémorisé dans une mémoire 18 du dispositif d'identification pour être ensuite envoyé vers le véhicule suivant la flèche 9 sous la forme d'un signal ayant une longueur par exemple de 20 bits. Enfin, le signal reçu par la flèche 9 est comparé avec le signal reçu de la mémoire 8 du véhicule dans un comparateur 10. Si ces deux signaux correspondent, sous réserve des retards dus au temps de réponse du matériel et de la transmission du signal dans la zone autorisée, le reste de la communication est autorisé et l'unité centrale du véhicule pourra, le cas échéant, commander la condamnation ou la décondamnation des serrures des ouvrants du véhicule. Bien entendu, un autre protocole de cryptage pourra être utilisé pour sécuriser la transmission des données.

[0006] Toutefois, malgré ce protocole de cryptage, il existe une façon de pirater le système, sans connaître ni la clé secrète, ni les différentes fonctions associatives du protocole d'encryptage. Ce procédé de piratage est représenté sur la figure 2. Selon ce procédé, on suppose que l'utilisateur U qui porte le dispositif d'identification I est situé à une distance du véhicule V supérieure à la distance autorisée de communication, par exemple de 10 à 100 m de distance du véhicule. Dans ce cas, un pirate équipé d'un premier boîtier relais 20 peut s'approcher du véhicule V à une distance suffisante pour communiquer avec celui-ci, par exemple à une distance de l'ordre de 1 à 5 m. Ce pirate actionne le début de la communication, par exemple en tirant sur la poignée extérieure de portière. Ceci déclenche l'émission des signaux basse fréquence par le véhicule vers le boîtier relais 20, comme indiqué par la flèche en zig-zag 21. Ce signal 21 envoyé par le véhicule est reçu par une bobine 22 du boîtier relais 20, qui est reliée à un récepteur 23 à 125 kHz. Ce récepteur 23 est relié à un émetteur à large bande à haute fréquence, de l'ordre de plusieurs MHz. L'émetteur 24 émet via son antenne 25, comme représenté par la flèche 26, vers un deuxième boîtier relais 30, qui est porté par un autre pirate qui suit de près l'utilisateur U. L'échange d'informations entre les deux boîtiers relais 20 et 30 s'effectuant à très haute fréquence, il est possible d'effectuer cette communication à grande distance. Le deuxième boîtier relais 30 comporte une antenne 31 pour recevoir le signal 26 émis par le boîtier relais 20. L'antenne 31 est reliée à un récepteur large bande à la même fréquence que l'émetteur 24 du premier boîtier relais 20. Le signal ainsi reçu est retransmis à basse fréquence à 125 kHz par un émetteur 33 qui est relié à une bobine d'émission 34 afin d'envoyer un signal 35 vers le dispositif d'identification I qui soit conforme au signal 21 émis par le véhicule. Le signal 35 étant la répétition du signal authentique du véhicule, le dispositif d'identification I va le reconnaître et émettre à son tour son signal de réponse 36, ledit signal de réponse 36 étant envoyé à haute fréquence et reçu par une antenne 37 du deuxième boîtier relais 30, par exemple à 434 MHz. L'antenne 37 est reliée à un récepteur 38, qui va convertir le signal à 434 MHz en un signal à une fréquence différente, par exemple à 315 MHz. Le signal est alors émis par un émetteur à large bande 39 via une antenne 40 vers le premier boîtier relais 20, cette différence de fréquence étant nécessaire pour que les différents signaux n'interfèrent pas entre eux. Bien entendu, la fréquence du signal 41 émis en retour par le deuxième boîtier relais 30 est différente à la fois de la fréquence du signal 26 et du signal 36. Ce signal 41 est capté par une antenne 27 du premier boîtier relais 20, ladite antenne 27 étant reliée à un récepteur large bande 28 de la même fréquence que l'émetteur 39. Le récepteur 28 est relié à un émetteur 29 qui transforme le signal à 315 MHz en un signal à 434 MHz qui est envoyé via l'antenne 42 du premier boîtier relais 20 vers le véhicule V, comme représenté par la flèche en zig-zag 43.

[0007] Il suffit que les pirates utilisent des boîtiers relais ayant des liaisons à large bande, par exemple supérieure à 50 MHz, ce qui est possible car les systèmes pirates n'ont pas à respecter les réglementations ; le temps de transit supplémentaire dû à la distance peut être alors de l'ordre de quelques nanosecondes, ce qui est négligeable en comparaison avec les constantes de temps nécessaires pour la transmission normale autorisée. A titre d'exemple, la communication totale peut être de l'ordre de 20 à 40 ms, et la durée totale du fonctionnement du système pour déclencher la décondamnation ou la condamnation des serrures électriques peut être de l'ordre de 100 ms.

[0008] Pour détecter un tel piratage et interrompre la communication, une solution pourrait consister à mesurer le temps de propagation des ondes radio UHF, en comparant ce temps mesuré avec un temps prédéterminé correspondant à une communication dans une zone limitée autorisée autour du véhicule. Toutefois, pour détecter le temps de retard dû à la distance, par rapport à un temps de communication global, il est nécessaire de disposer de large bande passante, ce qui correspond à une cadence de communication rapide, par exemple de l'ordre de 20 à 40 Mb/s. Avec une telle cadence de communication, il est nécessaire d'opérer à très haute fréquence, par exemple à 2,4 GHz. Mais pour mesurer des temps très courts, il est nécessaire d'avoir une bande passante très importante, ce qui vient se heurter aux réglementations applicables qui limitent fortement les bandes passantes autorisées, pour éviter une saturation de l'environnement par des ondes électromagnétiques.

[0009] L'invention a pour but d'éliminer les inconvénients précités et de proposer un système d'accès dit mains libres pour véhicule automobile, permettant de détecter un piratage du système, notamment par l'intermédiaire de boîtiers relais, en prenant compte du temps de propagation du signal entre le véhicule et le dispositif d'identification.

[0010] A cet effet, l'invention a pour objet un système d'accès dit mains libres pour véhicule automobile, comportant un dispositif d'identification destiné à être porté par un utilisateur et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique, ledit système étant apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, caractérisé par le fait que ladite unité centrale est apte à engendrer, lors de la communication, un train de bits d'anti-piratage, chaque bit dudit train étant émis vers le dispositif d'identification sous la forme d'un signal radio-fréquence représentatif dudit bit, de façon que lorsque le dispositif d'identification reçoit

ledit signal, ce dernier est réémis par le dispositif d'identification avec un temps de retard supérieur ou égal au temps d'émission utile du bit, et que la réception par l'unité centrale de commande dudit signal réémis déclenche l'émission par l'unité centrale du signal représentatif du bit suivant dans ledit train, le nombre de bits émis ou reçus dudit train, étant compté par un compteur de l'unité centrale, de façon que celle-ci compare ledit nombre et la durée réelle correspondant à l'émission ou à la réception dudit nombre de bits, afin de déterminer, au-delà d'une valeur de seuil prédéterminée, une tentative de piratage provoquant l'arrêt de ladite communication. On entend par "temps d'émission utile" le temps d'émission de l'information binaire dudit bit par rapport au temps total de la cellule à laquelle est associé ledit bit qui comprend généralement ledit temps utile et un temps de silence pour permettre la réception du signal réémis par le dispositif d'identification pendant ledit temps de silence.

[0011] Avantageusement, ladite valeur de seuil prédéterminée est donnée par une fenêtre de temps qui correspond à la durée totale théorique d'émission du train de bits d'anti-piratage, lorsque le dispositif d'identification est à une distance inférieure ou égale à la distance limite prédéterminée. Cette fenêtre de temps est une constante précise engendrée par exemple par un oscillateur piloté par quartz associé à un compteur sous contrôle du micro-contrôleur qui indique le nombre de périodes à compter. L'unité centrale de commande est apte à déterminer ladite tentative de piratage lorsque le nombre total de bits du train d'anti-piratage n'a pas été émis ou reçu par l'unité centrale de commande dans ladite fenêtre.

[0012] Selon une autre caractéristique, l'unité centrale peut comporter en mémoire une table de correspondance à double entrée, à savoir le nombre de bits émis et la durée d'émission réelle correspondante, pour donner en sortie la distance réelle entre le dispositif d'identification et l'unité centrale, les données de ladite table étant préalablement acquises par expérimentation et pouvant être périodiquement réactualisées, lorsque l'utilisateur portant le dispositif d'identification est assis sur le siège conducteur du véhicule, la distance du dispositif d'identification à l'unité centrale du véhicule étant alors sensiblement constante.

[0013] A titre d'exemple, le comptage du nombre de bits émis est arrêté lorsque l'unité centrale détecte la réception du dernier bit du train d'anti-piratage.

[0014] De préférence, le dispositif d'identification comporte une ligne à retard analogique pour réémettre le signal reçu du véhicule vers le véhicule avec un temps de retard prédéterminé.

[0015] Selon une autre caractéristique, l'unité centrale de commande comporte un oscillateur générateur d'ondes porteuses en radio fréquence, relié à un modulateur de phase, qui est commandé par le train de bits d'anti-piratage engendré par l'unité centrale du véhicule.

[0016] Selon encore une autre caractéristique, le train de bits d'anti-piratage est engendré par l'unité centrale après l'émission des données d'authentification cryptées vers le dispositif d'identification. Dans ce cas, le dispositif d'identification peut comporter un inverseur de phase pour inverser sélectivement la phase du signal représentatif des bits d'anti-piratage reçu par le dispositif d'identification en provenance du véhicule, ledit inverseur étant commandé, pour chaque bit d'anti-piratage, par un signal numérique d'authentification crypté de réponse du dispositif d'identification, à une cadence plus lente que celle du train de bits d'anti-piratage.

[0017] On peut prévoir alors que l'unité centrale du véhicule comporté un démodulateur de phase pour démoduler le signal reçu par le véhicule en provenance du dispositif d'identification, une porte logique OU exclusif dont les entrées sont reliées respectivement audit démodulateur de phase et à un retardateur de signal numérique, ledit retardateur étant apte à retarder d'un temps bit utile chaque bit du train d'anti-piratage engendré par l'unité centrale, ladite porte logique étant apte à délivrer en sortie un signal numérique représentatif du signal crypté de réponse du dispositif d'identification.

[0018] Dans une première forme de réalisation, le signal délivré en sortie de la porte logique OU exclusif précitée est comparé par l'unité centrale à un signal numérique crypté d'authentification engendré par l'unité centrale, afin d'authentifier le dispositif d'identification.

[0019] Dans une autre forme de réalisation, la sortie de ladite porte logique OU exclusif est reliée à une entrée d'une deuxième porte logique OU exclusif dont l'autre entrée reçoit un signal numérique crypté d'authentification engendré par l'unité centrale, afin de délivrer en sortie un signal représentatif des décalages temporels successifs de chaque bit du train d'anti-piratage, ce dernier signal étant reçu à l'entrée d'un intégrateur pour faire la somme des temps de réponse liés à chaque créneau de décalage de bit d'anti-piratage, la sortie dudit intégrateur étant reliée à un comparateur pour comparer ladite somme de temps de réponse avec une valeur de durée limite prédéterminée, au-delà de laquelle est détectée une tentative de piratage.

[0020] Avantageusement, on peut prévoir que le signal en provenance du dispositif d'identification est reçu par l'unité centrale et transmis à l'entrée d'un détecteur d'enveloppe pour détecter le front montant dudit signal, la détection de ce front montant étant apte à déclencher, d'une part, l'incrémentation d'une unité du compteur de nombre de bits et, d'autre part, l'émission du bit suivant dans le train de bits d'anti-piratage, après une durée prédéterminée qui correspond à un temps bit utile éventuellement augmenté d'un temps supplémentaire pour éviter toute interférence entre l'émission et la réception du signal par l'unité centrale.

[0021] Dans ce cas, on peut prévoir que l'unité centrale comporte un modulateur dit tout ou rien pour faire basculer l'unité centrale dans le mode émission ou réception des signaux vers ou en provenance du dispositif

d'identification, ledit modulateur tout ou rien étant commandé par la détection du front montant du signal reçu en provenance du dispositif d'identification.

[0022] Avantageusement, le dispositif d'identification comporte un récepteur pour recevoir des signaux d'éveil à faible cadence, ce récepteur comprenant successivement un détecteur d'enveloppe statique radio-fréquence à faible seuil et un amplificateur basse fréquence.

[0023] A titre d'exemple, le temps bit utile peut être compris entre 50 et 200 ns.

[0024] L'invention sera mieux comprise, et d'autres buts, détails, caractéristiques et avantages de celle-ci apparaîtront plus clairement au cours de la description explicative détaillée qui va suivre d'un mode de réalisation particulier de l'invention, donné uniquement à titre illustratif et non limitatif, en référence au dessin schématique annexé, dans lequel :

- la figure 1 est un schéma synoptique fonctionnel représentant le protocole d'encryptage pour sécuriser la transmission bidirectionnelle de données entre un véhicule et un dispositif d'identification ;
- la figure 2 est un schéma synoptique fonctionnel illustrant un moyen de piratage du système d'encryptage par l'intermédiaire de deux boîtiers relais ;
- la figure 3 est un schéma synoptique fonctionnel simplifié d'un système d'accès mains libres conforme à l'invention ;
- la figure 4 est un schéma synoptique fonctionnel plus détaillé correspondant au schéma de la figure 3 ;
- la figure 5 représente plusieurs chronogrammes illustrant les trames complètes d'interrogation émises par le véhicule et reçues en réponse par le véhicule ;
- la figure 6 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 5, indiquée par la flèche VI, correspondant au début de la séquence d'anti-piratage ;
- la figure 7 reprend les deux premiers chronogrammes de la figure 5 ;
- la figure 8 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 7, indiquée par la flèche VIII, au cours de la séquence d'anti-piratage ; et
- la figure 9 est une vue partielle et agrandie d'une portion des chronogrammes de la figure 5, indiquée par la flèche IX, et correspondant à la fin de la procédure d'anti-piratage.

[0025] On va maintenant se référer aux figures 3 et 4, qui représentent le système d'accès mains libres selon l'invention respectivement sous forme simplifiée et plus détaillée.

[0026] Le véhicule automobile V comporte dans son unité centrale un micro-contrôleur 50, qui est généralement dans un état de semi-sommeil ou d'attente d'un réveil. Lorsque l'utilisateur actionne la poignée extérieure de porte, un signal d'activation est envoyé au micro-contrôleur 50, comme indiqué par la flèche 51. En réponse, le micro-contrôleur envoie un signal d'alimentation général, comme représenté par la flèche 52, pour alimenter les différents composants électroniques de l'unité centrale. Puis, le micro-contrôleur 50 engendre une série de signaux à faible cadence sk, par exemple de l'ordre de 2 à 100 Kb/s sur la ligne V5. Les données véhiculées sur la ligne V5 sont successivement un signal d'éveil e, un signal représentatif d'un nombre aléatoire R d'une longueur par exemple de 56 bits, un signal représentatif de la fonction f (R,K) d'une longueur par exemple de 28 bits, et d'un signal représentatif de données de service s, par exemple d'une longueur de 100 à 5 000 bits, par exemple des données sur la maintenance, le réglage du véhicule, etc (voir figure 5). La ligne V5 est reliée à un émetteur 53 pour émettre via une antenne 54 les signaux vers le dispositif d'identification I comme représenté par la flèche E. L'émetteur 53 comporte, comme mieux visible sur la figure 4, un oscillateur 55 pour engendrer une onde porteuse à ultra haute fréquence, ledit oscillateur étant alimenté par la ligne 52. L'oscillateur 55 est relié à un modulateur de phase 56, qui est à son tour relié à un modulateur tout ou rien 57, ce dernier ayant une entrée reliée à la ligne V5 et sa sortie reliée à l'antenne 54 précitée. Lors de l'émission des données à faible cadence sk sur la ligne V5, le modulateur de phase est inactif. Le modulateur tout ou rien 57 est destiné à alternativement permettre l'émission d'un signal et la réception d'un signal par l'unité centrale du véhicule, comme expliqué plus loin. A titre d'exemple, l'amplitude du signal émis est de l'ordre de 2 V efficace.

[0027] Le signal émis E est reçu par une antenne 100 du dispositif d'identification I avec une atténuation de l'ordre de -40 dBm, ce qui représente un coefficient d'atténuation de 100 fois, c'est à dire que le signal reçu par le dispositif d'identification présente une amplitude de l'ordre de 20 mV. L'antenne 100 est reliée à un filtre radio-fréquence 101 (uniquement représenté sur la figure 4) pour éliminer les fréquences parasites. La sortie du filtre 101 est reliée à un embranchement, d'une part, vers un récepteur à faible cadence et à faible consommation 102 et, d'autre, part à une ligne à retard analogique 103. Les signaux à faible cadence sk ne sont pas transmis par la ligne à retard 103, mais passent essentiellement via le récepteur 102. Comme mieux visible sur la figure 4, le récepteur 102 comprend successivement un détecteur d'enveloppe radio-fréquence 104 pour reconstituer les signaux à faible cadence sur la ligne I5, qui correspondent à ceux de la ligne V5. La sortie du détecteur d'enveloppe 104 est reliée à un amplificateur basse fréquence 105, dont la sortie est reliée en parallèle, d'une part, à un décodeur de séquence d'éveil 106 et, d'autre part, à un micro-contrôleur 107 du dispositif d'identification I via une ligne 108. Au démarrage de la communication avec le véhicule, seul le décodeur 106 est alimenté en permanence par la pile du dispositif

d'identification. Autrement dit, les données d'éveil e sont décodées par le décodeur 106, afin d'envoyer un ordre d'éveil au micro-contrôleur 107, à la sortie du décodeur 106. Le micro-contrôleur 107 éveille alors tous les autres composants électroniques du dispositif d'identification. Ainsi, les données suivantes, à savoir les signaux R, f et s, sont transmis directement au micro-contrôleur 107 via la ligne en parallèle 108.

[0028] Après émission des données de service s, le micro-contrôleur 50 du véhicule V engendre des bits d'anti-piratage h à la cadence lente sk du micro-processeur, lesdits bits d'anti-piratage étant reçus par une mémoire tampon à générateur de séquences binaires aléatoires 58, pour délivrer en sortie les bits d'anti-piratage à haute cadence fk, sur une ligne V7. La sortie de la mémoire tampon 58 est reliée à un embranchement, d'une part, avec le modulateur de phase 56 pour moduler en phase l'onde porteuse engendrée par l'oscillateur 55, et d'autre part, avec un retardateur numérique d'un temps bit utile 59, dont la fonction sera expliquée plus loin. Chaque bit d'anti-piratage est transmis sous la forme d'un signal radio-fréquence via l'antenne 54 en direction du dispositif d'identification I. La trame globale d'émission V2 des signaux par l'antenne 54 est illustrée sur les figures 5 et 7. En se référant plus particulièrement à la figure 6, on a représenté le début de la trame d'interrogation des bits d'anti-piratage h sur la ligne V2. Sur la ligne V2 de la figure 6, on constate que chaque bit d'anti-piratage est porté par une onde oscillante à très haute fréquence ayant un temps bit Tb compris par exemple entre 50 et 200 ns. L'émission des bits d'anti-piratage h1, h2...hn est autorisée par le modulateur tout ou rien 57, en fonction d'un signal de commande V1 qui est émis par une unité de gestion de base de temps 60 du véhicule V, laquelle unité 60 est apte à délivrer les signaux d'horloge à faible cadence sk, à moyenne cadence mk et à haute cadence fk. Bien entendu, l'unité 60 est reliée au micro-contrôleur 50, comme indiqué par la double flèche 61. La génération du signal V1 sera expliquée plus loin.

[0029] Le dispositif d'identification I reçoit via son antenne 100 sur la ligne I1 (voir figure 6) un signal qui correspond au bit d'anti-piratage h1 émis par le véhicule V, avec un temps retard δ qui correspond au temps de propagation du signal entre le véhicule et le dispositif d'identification. Le signal passe alors par la ligne à retard analogique 103, qui peut par exemple être constituée par un bobinage en cuivre, ce qui permet de réduire la consommation d'énergie par le dispositif d'identification, car cette ligne à retard n'a pas besoin d'être alimentée en énergie. On a représenté sur la figure 8 le signal I2v qui correspond au signal virtuel en sortie de la ligne à retard analogique 103, c'est à dire à l'enveloppe dudit signal analogique, ledit signal étant retardé d'une durée prédéterminée Dℓ. La sortie de la ligne à retard 103 est reliée à l'entrée d'un inverseur de phase 109 pour inverser la phase du signal analogique transmis par la ligne à retard 103, en fonction d'un signal de commande crypté d'authentification g, dont la trame est représentée sur la ligne I6. Comme visible sur la ligne I6 représentée sur la figure 8, la cadence des bits du signal g est à moyenne cadence mk, plus faible que la haute cadence fk des bits d'anti-piratage h. A cet effet, on prévoit que le micro-contrôleur 107 du dispositif d'identification transmet à faible cadence sk le signal g à une mémoire tampon 110 qui délivre en sortie le signal g à la cadence moyenne mk vers l'inverseur de phase 109.

[0030] L'inverseur de phase 109 délivre en sortie un signal analogique, dont le signal virtuel est représenté en I7v qui représente l'enveloppe dudit signal. La sortie de l'inverseur de phase 109 est reliée à un amplificateur 111 ayant un gain de + 20 dB pour émettre le signal avec une amplitude de l'ordre de 200 mV. Ce signal amplifié est représenté sur la ligne I4 et correspond au bit d'émission h1 avec le retard δ dû à la propagation du signal et au retard analogique Dℓ dû à la ligne à retard 103. Ce signal 14 est réémis par une antenne 112 vers le véhicule V, comme représenté par la flèche RE. Lors de la réception du premier bit d'anti-piratage h1 par le dispositif d'identification, ce premier bit d'anti-piratage va déclencher la génération du signal crypté d'authentification g par le dispositif d'identification en vue de commander l'inverseur de phase 109. A cet effet, la sortie de l'amplificateur 111 est reliée également à une ligne de déclenchement 113 qui comporte en série une diode 114 et un déclencheur 115 pour activer une unité de gestion de temps de base 116 qui délivre des signaux d'horloge à faible cadence sk et à moyenne cadence mk, ladite unité 116 étant reliée au micro-contrôleur 107, comme indiqué par la double flèche 117.

[0031] En partant de l'hypothèse que les signaux électromagnétiques transmis se propagent à la vitesse de la lumière, à savoir 3.10^8 m/s, on peut considérer que la durée de transmission des signaux est de l'ordre de 3 ns par mètre de distance entre le véhicule et le dispositif d'identification I. Autrement dit, pour un trajet aller-retour entre le véhicule V et le dispositif d'identification I, espacé d'une distance d'environ 5 mètres, la durée de propagation δ serait de l'ordre de 30 ns. A cette durée de propagation δ, on pourrait ajouter le temps de réponse des circuits électroniques, qui pourrait être de l'ordre de quelques ns ou dizaines de ns, selon la bande passante attribuée à la porteuse.

[0032] Le signal réémis RE par le dispositif d'identification est reçu par un récepteur 62 via une antenne 63, avec une atténuation de l'ordre de - 40 dBm, ce qui représente un coefficient d'atténuation de 100 fois, c'est à dire que le signal reçu par le véhicule présente une amplitude de l'ordre de 2 mV. Comme mieux représenté sur la figure 4, le récepteur 62 comporte un filtre radio-fréquence 64 relié à l'antenne 63, dont le signal de sortie est représenté par la ligne V3, ce signal étant délivré à l'entrée d'un amplificateur logarithmique 65 qui présente un gain de 80 dB, ce qui permet d'atteindre un coefficient de multiplication allant jusqu'à 10 000 fois, et notam-

ment de délivrer en sortie dudit amplificateur 65 un signal de l'ordre de 2V efficace. L'amplificateur 65 est relié en sortie à un embranchement entre, d'une part, un démodulateur d'amplitude 66, qui permet de détecter l'enveloppe du signal reçu, et, d'autre part, un démodulateur de phase 67. Le détecteur d'enveloppe 66 délivre en sortie un signal numérique représenté sur la ligne V4, ledit signal étant délivré à l'entrée de l'unité de gestion de base de temps 60 précitée. A la réception du bit d'anti-piratage reçu en retour, l'unité de gestion de base de temps 60 déclenche l'émission du bit d'anti-piratage suivant h2 avec un décalage correspondant au temps bit utile Tb + ε,ε correspondant à un faible retard de sécurité afin d'éviter tout chevauchement entre l' émission et la réception des signaux par le véhicule. Ainsi, la réception du bit d'anti-piratage en retour par le véhicule déclenche le coup d'horloge suivant à la cadence fk ainsi que le basculement du modulateur tout ou rien 57, via la ligne V1. Bien entendu, on pourrait également prévoir que le petit retard ε soit proche de 0s.

[0033] Chaque nouveau coup d'horloge à la cadence fk déclenché par la réception du bit d'anti-piratage précédent, provoque l'incrémentation d'une unité dans un compteur 68, lequel compteur 68 compte le nombre de bits reçus en fonction du temps. Toutefois, comme la réception d'un bit déclenche l'émission d'un bit d'anti-piratage suivant, on peut aussi bien compter directement le nombre de bits d'anti-piratage émis en fonction du temps. Lorsque la fin réelle du train de bits d'anti-piratage est détectée par l'unité centrale du véhicule, l'unité 60 envoie un signal Fr pour arrêter le comptage des bits d'anti-piratage et pour provoquer l'envoi par le compteur 68 d'un signal représentatif du nombre de bits comptés au micro-contrôleur 50, comme indiqué par la flèche 69. Si la fin réelle Fr est comprise dans la fenêtre de réception maximale Fm, comme indiqué à la figure 5, cela signifie que la transmission n'a pas été piratée. En fonction du nombre de bits, le micro-contrôleur 50 peut calculer la distance réelle entre le véhicule V et le dispositif d'identification I, en fonction d'une table de correspondance préalablement mémorisée. Si cette distance dépasse la distance autorisée, la communication est interrompue comme étant le résultat d'une tentative de piratage ou tout simplement comme étant une communication à trop grande distance du véhicule.

[0034] Ce compteur permet ainsi de détecter un piratage utilisant des boîtiers-relais entre le véhicule et le dispositif d'identification. Toutefois, un pirate pourrait essayer de piéger ce système en anticipant sur le signal devant être émis par le dispositif d'identification. A titre d'exemple, dès que le pirate détecte avec un boîtier-relais l'émission par le véhicule d'un bit d'anti-piratage, il peut provoquer l'émission anticipée d'un signal-talon, en préambule à la réémission du signal retardé par la ligne à retard du dispositif d'identification. Avantageusement, ce signal-talon aurait une durée qui correspondrait à la durée de propagation du signal sur la distance supplémentaire entre le dispositif d'identification et le véhicule, par rapport à la distance maximale autorisée. Ainsi, le détecteur d'enveloppe 66 du véhicule V détecterait, en premier lieu, la réception de ce signal-talon, provoquant à son tour l'émission anticipée du second bit d'anti-piratage.

[0035] Le système selon l'invention permet également, grâce au compteur 68, de déterminer si le nombre total de bits d'anti-piratage a bien été reçu pendant une fenêtre de réception maximale Fm, représentée sur la figure 5. Les chronogrammes des figures 5 à 9 correspondent à une transmission non piratée du signal. La fin réelle Fr de la réception du train de bits d'anti-piratage est, sur ces figures, bien située dans la fenêtre maximale de réception Fm, comme représenté sur la figure 5. La durée totale Tt de réception des bits d'anti-piratage est calculée selon la formule suivante : Tt = n(Dℓ + Tb + ε + 2 δ). Ainsi, on constate qu'avec un train de n bits d'anti-piratage, on multiplie par la variable n la durée de propagation 2δ qui est fonction directe de la distance entre le dispositif d'identification et le véhicule. Ainsi, s'il est difficile de détecter avec des circuits électroniques à faible coût des durées de l'ordre de quelques dizaines de ns, il est beaucoup plus facile de détecter des durées de l'ordre de n x quelques dizaines de ns, c'est à dire des durées de l'ordre de la ms. Toutefois, si le pirate anticipe sur la réémission du signal par le dispositif d'identification, la variable 2n δ restera dans la limite acceptable et ainsi le système ne pourra pas détecter le piratage.

[0036] A cet effet, on peut prévoir, en alternative ou en supplément, une autre façon de calculer le temps de retard dû à la propagation du signal.

[0037] Le démodulateur de phase 67 délivre un signal représentatif de la fonction goh sur la ligne V9 qui est reliée à une entrée d'une porte logique OU exclusif 70. Cette porte logique 70 reçoit sur son autre entrée un signal V8 représentatif de la fonction h, délivré en sortie du retardateur numérique 59. La porte logique 70 pourrait être remplacée par un autre type de mélangeur, comme représenté sur la figure 3. Le signal V8 correspond au signal V7 avec un retard correspondant au décalage Dℓ du retardateur analogique 103 du dispositif d'identification I. La porte logique 70 délivre en sortie un signal V10, qui est représentatif du décalage entre les signaux V8 et V9, c'est à dire un signal représentatif du signal encrypté d'authentification g émis par le dispositif d'identification I, avec un petit décalage correspondant au temps de propagation du signal qui est égal à 2 δ, comme visible sur la figure 8.

[0038] La sortie de la porte logique 70 est reliée à un embranchement entre, d'une part, un filtre passe-bas 71 à la cadence moyenne mk qui est la cadence correspondant au signal g et, d'autre part, une autre porte logique OU exclusif 73. Le filtre passe-bas 71 est relié à une mémoire tampon 72, qui transforme ledit signal de la cadence mk à la cadence sk avant de l'envoyer au micro-contrôleur 50 qui va comparer le signal g reçu en provenance du dispositif d'authentification avec le si-

gnal g engendré au niveau du véhicule, en vue de l'authentification de la communication, ce qui correspond à la dernière étape 10 illustrée sur le schéma de la figure 1.

[0039] Le micro-contrôleur 50 délivre le signal g propre au véhicule à une mémoire tampon 74 à la cadence sk, afin qu'il la renvoie à la cadence mk à l'autre entrée de la porte logique 73 précitée. On a représenté sur la ligne V11 le signal g qui correspond exactement au signal g engendré par le dispositif d'identification et émis sur la ligne I6, comme représenté sur la figure 8. La porte logique 73 mélange les signaux V10 et V11 afin de ne délivrer en sortie que les décalages dus au temps de propagation du signal entre le véhicule V et le dispositif d'identification I, comme représenté sur la ligne V12. La sortie de la porte logique 73 est reliée à l'entrée d'un intégrateur 75, qui va délivrer en sortie un signal V13 qui va monter par escalier en fonction du temps, pour chaque créneau C représentatif du temps de propagation du signal. La ligne V13 est reliée à l'entrée d'une unité 76 recevant sur une autre entrée une valeur limite de seuil 77 qui correspond à un temps de propagation total maximal acceptable $n \times 2\delta \leq T$ max, avec δ correspondant au temps de propagation sur une distance autorisée. Selon que l'amplitude du signal de sortie sur la ligne V13 est supérieure ou non à cette valeur limite 77, un signal de tentative de piratage sera envoyé ou non via la ligne 78 au micro-contrôleur 50.

[0040] L'intégrateur 75 permet de détecter une tentative de piratage, même dans le cas où le pirate ajoute un talon d'anticipation au signal réémis par le dispositif d'identification. En effet, si ce signal-talon peut piéger le compteur 68, en revanche la porte logique 73 interprétera ce signal-talon comme un signal erroné au moins avec une chance sur deux, et donc délivrera en sortie un créneau équivalent à ce signal-talon, lequel créneau sera additionné par l'intégrateur 75 de la même façon que pour les retards dus au temps de propagation.

[0041] Enfin, le micro-contrôleur 50 peut délivrer différents signaux de sortie aux autres composants du véhicule par la voie 80 représentée sur les figures 3 et 4.

[0042] A titre d'exemple, la cadence d'horloge intermédiaire mk est entre 20 et 60 fois inférieure à la cadence fk.

[0043] En variante, on pourrait remplacer les antennes 54 et 63 du véhicule V par une antenne unique 82 représentée en traits interrompus sur la figure 4, laquelle antenne 82 serait reliée à un diplexeur 81 représenté en traits interrompus sur la figure 4, afin de commuter entre le mode de réception et le mode d'émission selon le cas. De manière analogue, on pourrait remplacer les antennes 100 et 112 du dispositif d'identification par une antenne unique 121 reliée à un diplexeur 120, représentés en traits interrompus sur la figure 4. Les diplexeurs 81 et 120 pourraient ainsi communiquer entre eux, comme indiqué par la double flèche T.

[0044] Dans une variante du mode de réalisation représenté à la fig ure 4, l'unité centrale est reliée à au moins deux, par exemple trois, antennes d'émission/réception telles que l'antenne unique 82, disposées en plusieurs points du véhicule V. Des mesures de distance sont alors réalisées séquentiellement entre le dispositif d'identification I et chacune des antennes d'émission/réception du véhicule V. Ces mesures de distance sont réalisées par l'intermédiaire de la durée de propagation δ des bits anti-piratage à l'aide de la table de correspondance susmentionnée. Dans cette variante, il est possible de localiser précisément, par exemple à quelques centimètres ou dizaines de centimètres près, la position du dispositif d'identification I par un calcul de triangulation effectué par l'unité centrale. Ceci permet en outre de prendre en compte la position du dispositif d'identification I par rapport au véhicule V, par exemple, de quelle portière il se trouve le plus proche, lors des prises de décision réalisées dans l'unité centrale pour commander la condamnation ou la décondamnation des serrures des ouvrants du véhicule. Cette variante peut évidemment aussi être réalisée avec des antennes d'émission et de réception séparées.

[0045] Dans tous les cas, la ligne à retard 103 du dispositif d'identification I permet de différer la réémission de chaque bit anti-piratage par rapport à sa réception afin d'utiliser une même fréquence radio pour la transmission des signaux correspondants dans le sens depuis le véhicule V vers le dispositif d'identification I (flèche E ou T) et dans le sens depuis le dispositif d'identification I vers le véhicule V (flèche RE ou T).

[0046] Comme visible sur la figure 5, sur la ligne V3, après la réception du signal hog, le véhicule V reçoit en provenance du dispositif d'identification un signal hos où s représente des données de service qui viennent moduler le signal h par inversion de phase, comme cela était le cas pour le signal g dont la longueur est inférieure à celle du signal h.

[0047] La séquence des bits anti-piratage h étant une séquence binaire aléatoire ou pseudo-aléatoire, elle entraîne un étalement du spectre des signaux radiofréquences utilisés pour la transmettre du véhicule vers le dispositif d'identification et inversement. Cet étalement de spectre est d'autant plus important que la cadence de modulation fk utilisée pour transmettre la séquence des bits anti-piratage h est élevée. Un tel étalement de spectre est connu pour être avantageux du point de vue de la robustesse du signal vis à vis des interférences et des échos multiples, ce qui facilite les transmissions multiples du signal, par exemple l'aller-retour du signal entre le véhicule et le dispositif d'identification. En revanche, la démodulation du signal crypté d'authentification g au niveau de l'unité centrale du véhicule est rendue d'autant plus difficile que le spectre du signal RE est étalé.

[0048] L'agencement de la ligne à retard 103 pour réémettre les bits anti-piratage h successifs retardés d'un temps bit utile en tant que modulation à cadence élevée fk du signal crypté d'authentification g, lui-même étant transmis à la cadence moyenne mk, permet d'as-

surer que la clé de démodulation correspondante, c'est-à-dire la même séquence aléatoire des bits anti-piratage h, est toujours disponible au niveau de l'unité centrale de commande lors de la réception du signal RE, ce qui permet de réaliser la démodulation du signal RE reçu indépendamment du degré d'étalement du spectre de ce signal.

[0049] En outre, la robustesse du système d'accès vis à vis des échos multiples, par exemple dans le cas où le signal E émis par l'unité centrale est reçu par le dispositif d'identification I sous la forme d'un signal transmis directement et d'un écho ayant subi une réflexion sur un obstacle, est assurée par le fait que le dispositif d'identification I réagit toujours au premier signal reçu, qui ne peut être que le signal transmis directement.

[0050] Bien que l'invention ait été décrite en liaison avec un exemple particulier de réalisation, il est bien évident qu'elle n'y est nullement limitée et qu'elle comprend tous les équivalents techniques des moyens décrits ainsi que leurs combinaisons si celles-ci entrent dans le cadre de l'invention.

Revendications

1. Système d'accès dit mains libres pour véhicule automobile (V), comportant un dispositif d'identification (I) destiné à être porté par un utilisateur (U) et apte à établir une communication bidirectionnelle à distance et sans fil avec une unité centrale de commande embarquée sur le véhicule, pour authentifier l'utilisateur et commander des moyens de condamnation/ décondamnation des serrures des ouvrants lorsque l'utilisateur a été reconnu authentique, ledit système étant apte à établir ladite communication bidirectionnelle lorsque le dispositif d'identification est situé à une distance inférieure à une distance limite prédéterminée du véhicule, **caractérisé par le fait que** ladite unité centrale est apte à engendrer, lors de la communication, un train de bits d'anti-piratage (h), chaque bit dudit train étant émis vers le dispositif d'identification (I) sous la forme d'un signal radio-fréquence représentatif dudit bit, de façon que lorsque le dispositif d'identification reçoit ledit signal, ce dernier est réémis par le dispositif d'identification avec un temps de retard (Dℓ) supérieur ou égal au temps d'émission utile (Tb) du bit, et que la réception par l'unité centrale de commande dudit signal réémis déclenche l'émission par l'unité centrale du signal représentatif du bit suivant dans ledit train, le nombre de bits émis ou reçus dudit train, étant compté par un compteur (68) de l'unité centrale, de façon que celle-ci compare ledit nombre et la durée réelle (Tt) correspondant à l'émission ou à la réception dudit nombre de bits, afin de déterminer, au-delà d'une valeur de seuil prédéterminée, une tentative de piratage provoquant l'arrêt de ladite communication.

2. Système selon la revendication 1, **caractérisé par le fait que** ladite valeur de seuil prédéterminée est donnée par une fenêtre de temps (Fm) qui correspond à la durée totale théorique d'émission du train de bits d'anti-piratage, lorsque le dispositif d'identification (I) est à une distance inférieure ou égale à la distance limite prédéterminée, et l'unité centrale de commande est apte à déterminer ladite tentative de piratage lorsque le nombre total de bits du train d'anti-piratage n'a pas été émis ou reçu par l'unité centrale de commande dans ladite fenêtre.

3. Système selon la revendication 1 ou 2, **caractérisé par le fait que** l'unité centrale comporte en mémoire une table de correspondance à double entrée, à savoir le nombre de bits émis et la durée d'émission réelle correspondante, pour donner en sortie la distance réelle entre le dispositif d'identification et l'unité centrale, les données de ladite table étant préalablement acquises par expérimentation et pouvant être périodiquement réactualisées.

4. Système selon l'une des revendications 1 à 3, **caractérisé par le fait que** le comptage du nombre de bits émis est arrêté lorsque l'unité centrale détecte la réception du dernier bit (hn) du train d'anti-piratage.

5. Système selon l'une des revendications 1 à 4, **caractérisé par le fait que** le dispositif d'identification (I) comporte une ligne à retard analogique (103) pour réémettre le signal reçu du véhicule (V) vers le véhicule avec un temps de retard prédéterminé (D ℓ).

6. Système selon l'une des revendications 1 à 5, **caractérisé par le fait que** l'unité centrale de commande comporte un oscillateur (55) générateur d'ondes porteuses en radio fréquence, relié à un modulateur de phase (56), qui est commandé par le train de bits d'anti-piratage (h) engendré par l'unité centrale du véhicule (V).

7. Système selon l'une des revendications 1 à 6, **caractérisé par le fait que** le train de bits d'anti-piratage (h) est engendré par l'unité centrale après l'émission des données d'authentification cryptées (R,f) vers le dispositif d'identification (I).

8. Système selon la revendication 7, **caractérisé par le fait que** le dispositif d'identification I comporte un inverseur de phase (109) pour inverser sélectivement la phase du signal représentatif des bits d'anti-piratage reçu par le dispositif d'identification en provenance du véhicule (V), ledit inverseur étant commandé, pour chaque bit d'anti-piratage, par un signal numérique d'authentification crypté (g) de réponse du dispositif d'identification, à une cadence

plus lente (mk) que celle (fk) du train de bits d'anti-piratage.

9. Système selon la revendication 8, **caractérisé par le fait que** l'unité centrale du véhicule (V) comporte un démodulateur de phase (67) pour démoduler le signal reçu par le véhicule en provenance du dispositif d'identification (I), une porte logique OU exclusif (70) dont les entrées sont reliées respectivement audit démodulateur de phase et à un retardateur de signal numérique (59), ledit retardateur étant apte à retarder d'un temps bit utile (Tb) chaque bit du train d'anti-piratage (h) engendré par l'unité centrale, ladite porte logique étant apte à délivrer en sortie un signal numérique (V10) représentatif du signal crypté de réponse du dispositif d'identification.

10. Système selon la revendication 9, **caractérisé par le fait que** le signal (V10) délivré en sortie de la porte logique OU exclusif (70) précitée est comparé par l'unité centrale à un signal numérique crypté d'authentification (g) engendré par l'unité centrale, afin d'authentifier le dispositif d'identification (I).

11. Système selon la revendication 9 ou 10, **caractérisé par le fait que** la sortie de ladite porte logique OU exclusif (70) est reliée à une entrée d'une deuxième porte logique OU exclusif (73) dont l'autre entrée reçoit un signal numérique crypté d'authentification (g) engendré par l'unité centrale, afin de délivrer en sortie un signal (V12) représentatif des décalages temporels successifs de chaque bit du train d'anti-piratage, ce dernier signal étant reçu à l'entrée d'un intégrateur (75) pour faire la somme des temps de réponse liés à chaque créneau (C) de décalage de bit d'anti-piratage, la sortie dudit intégrateur étant reliée à un comparateur (76) pour comparer ladite somme de temps de réponse avec une valeur de durée limite prédéterminée (77), au-delà de laquelle est détectée une tentative de piratage.

12. Système selon l'une des revendications 1 à 11, **caractérisé par le fait que** le signal en provenance du dispositif d'identification (I) est reçu par l'unité centrale et transmis à l'entrée d'un détecteur d'enveloppe (66) pour détecter le front montant dudit signal, la détection de ce front montant étant apte à déclencher, d'une part, l'incrémentation d'une unité du compteur de nombre de bits (68) et, d'autre part, l'émission du bit suivant dans le train de bits d'anti-piratage, après une durée prédéterminée qui correspond à un temps bit utile éventuellement augmenté d'un temps supplémentaire (ε) pour éviter toute interférence entre l'émission et la réception du signal par l'unité centrale.

13. Système selon la revendication 12, **caractérisé par le fait que** l'unité centrale comporte un modulateur (57) dit tout ou rien pour faire basculer l'unité centrale dans le mode émission ou réception des signaux vers ou en provenance du dispositif d'identification (I), ledit modulateur tout ou rien étant commandé par la détection du front montant du signal reçu en provenance du dispositif d'identification.

14. Système selon l'une des revendications 1 à 13, **caractérisé par le fait que** le dispositif d'identification comporte un récepteur (102) pour recevoir des signaux d'éveil (e) à faible cadence (sk), ce récepteur comprenant successivement un détecteur d'enveloppe statique radio-fréquence à faible seuil (104) et un amplificateur basse fréquence (105).

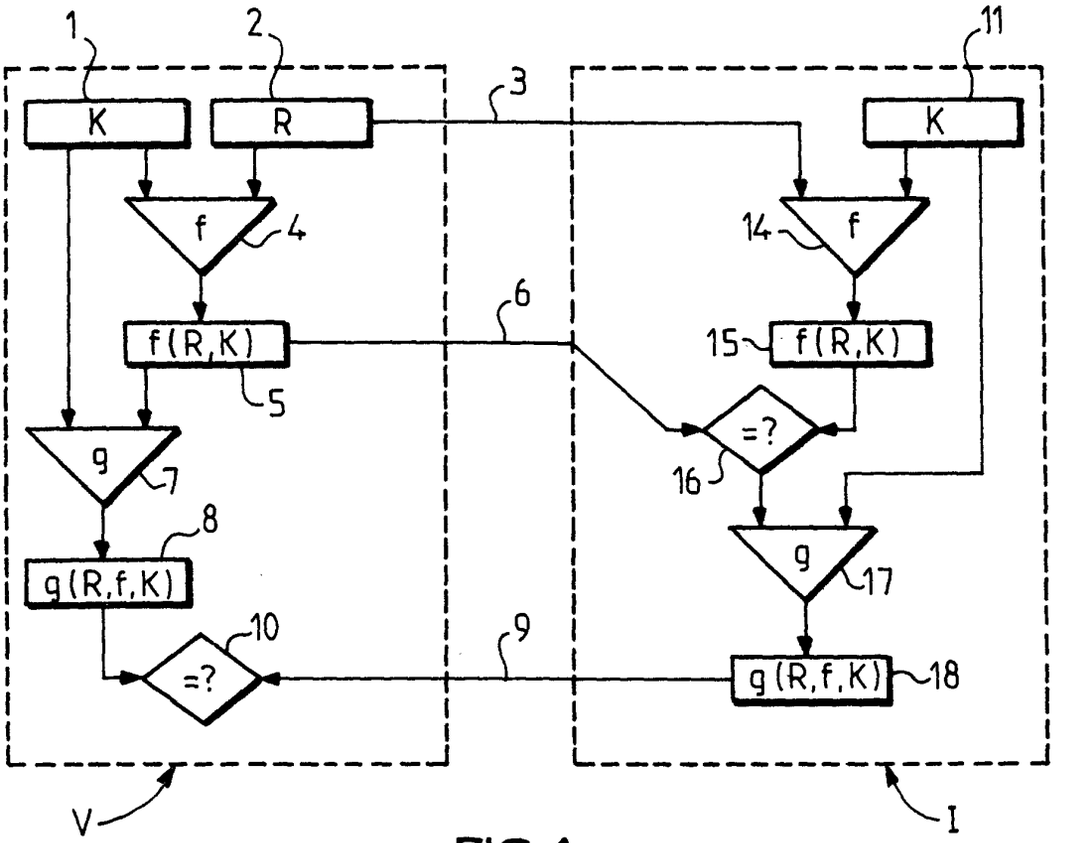
1
2
3
11
K
R
K
f
4
14
f
6
f(R,K)
5
15
f(R,K)
=?
16
g
7
8
g
17
g(R,f,K)
10
9
=?
g(R,f,K)
18
V
I

FIG.1

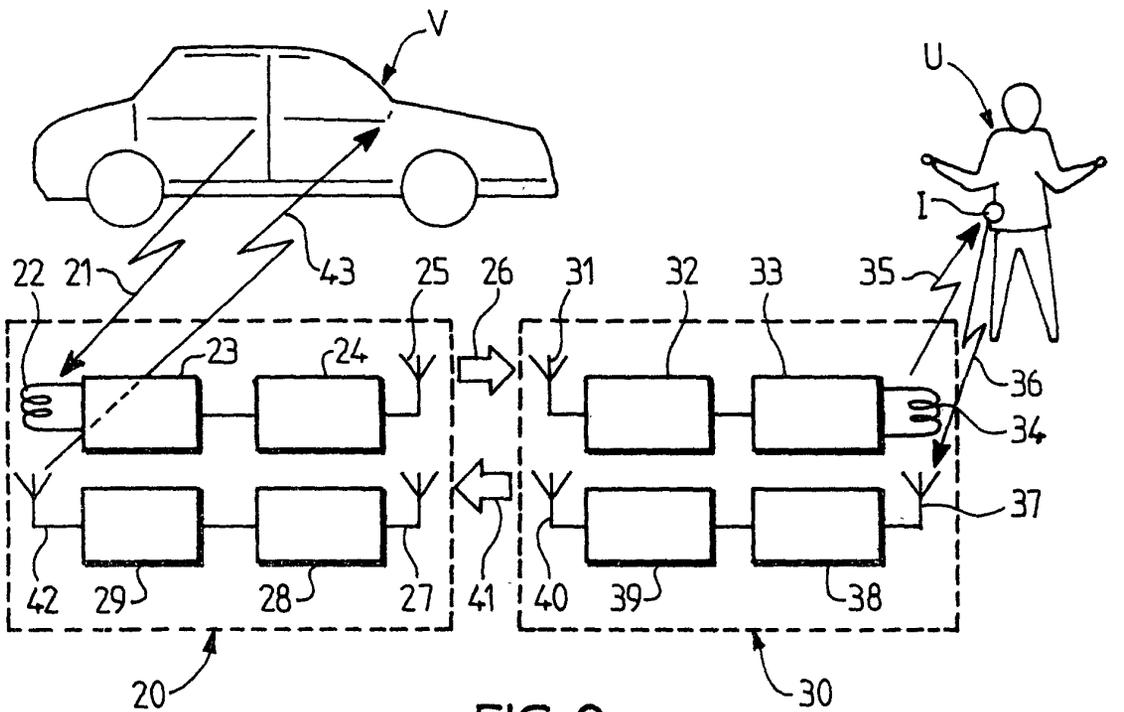
V
U
I
22
21
43
25
26
31
32
33
35
23
24
36
34
37
42
29
28
27
41
40
39
38
20
30

FIG.2

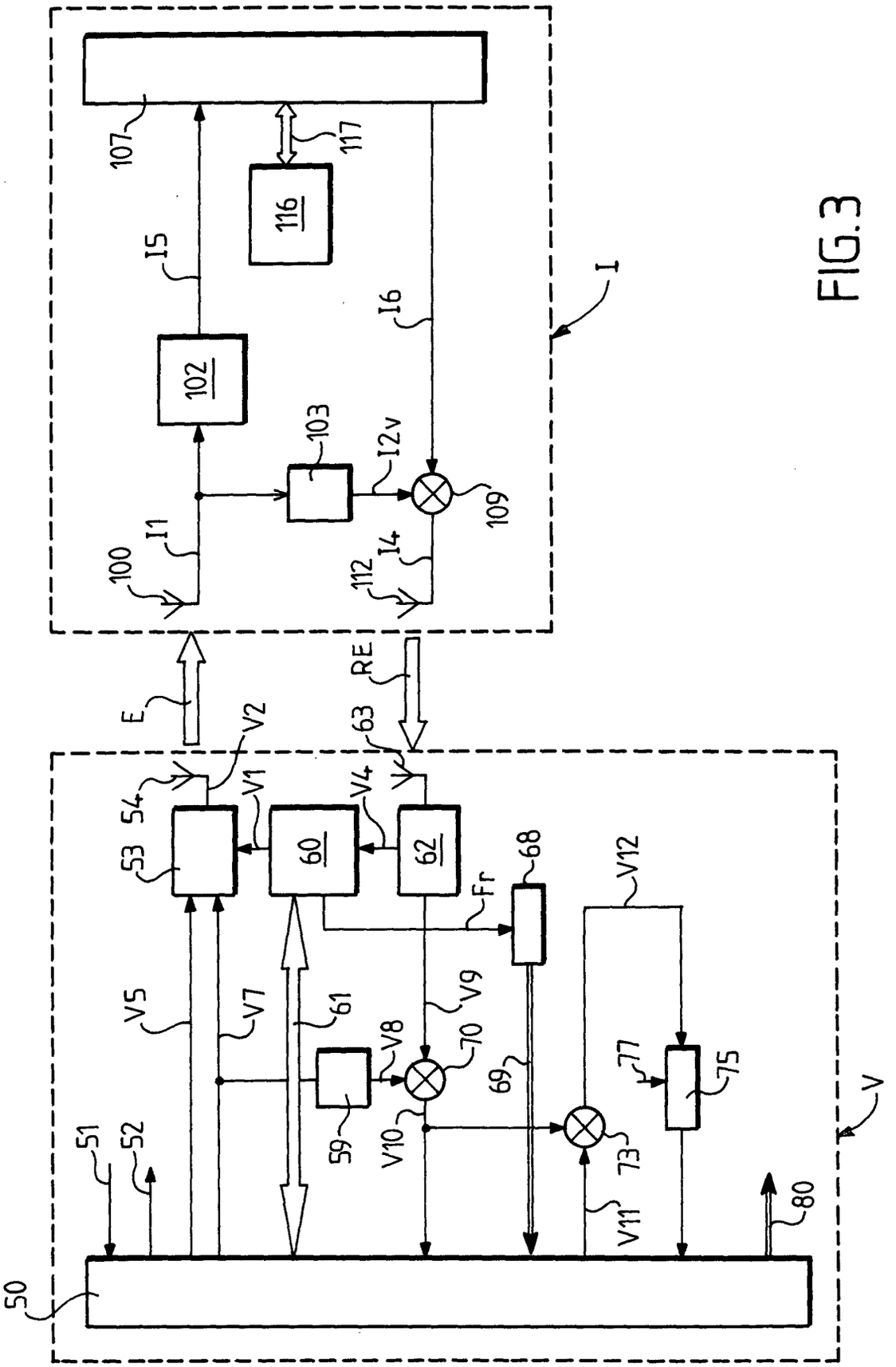
I
107
117
116
15
16
102
103
12v
109
11
100
14
112
RE
E
63
V2
54
V1
V4
53
60
62
68
Fr
V12
V5
V7
61
V9
V8
70
69
77
75
59
V10
73
V11
80
V
51
52
50

FIG.3

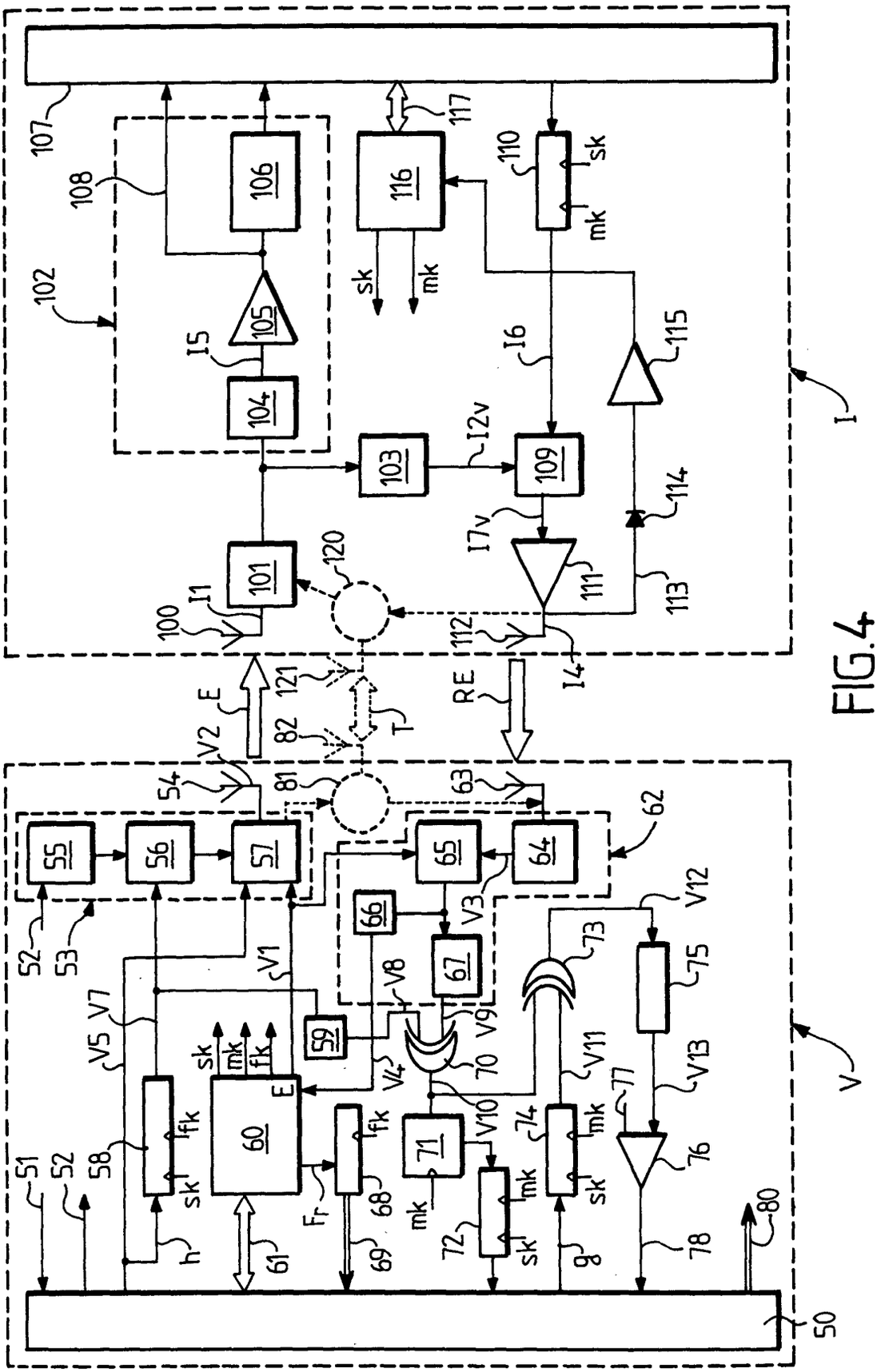
I
V
50
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
120
121
I1
I2v
I3
I4
I5
I6
I7v
E
T
RE
V1
V2
V3
V4
V5
V7
V8
V9
V10
V11
V12
V13
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
80
81
82
sk
mk
fk
Fr
h
g

FIG.4

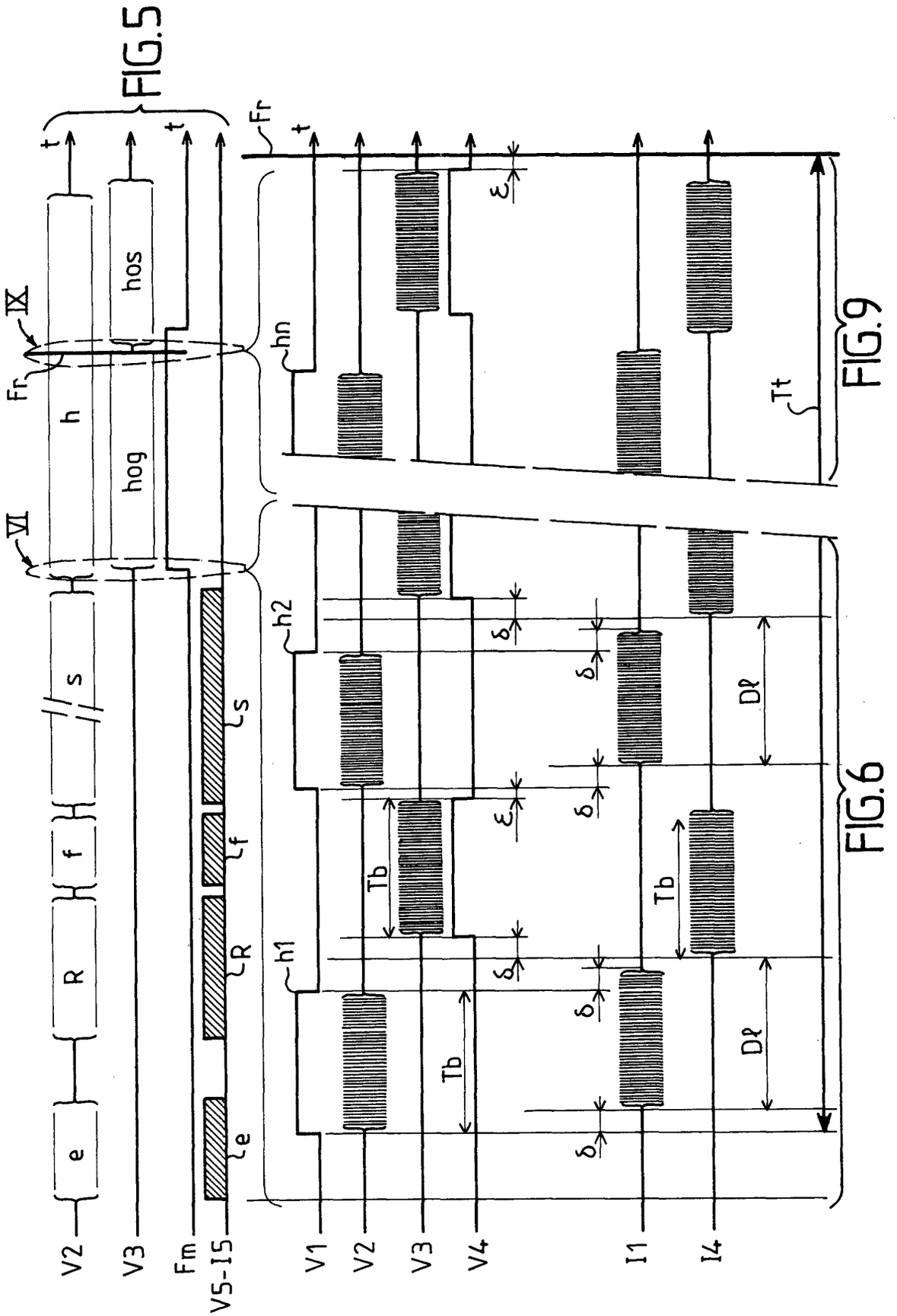
FIG.5
t
hos
h
hog
IX
VI
Fr
s
f
R
e
V2
V3
Fm
V5-15
FIG.9
Fr
t
hn
ε
Tt
FIG.6
h2
h1
δ
Tb
Dℓ
V1
V2
V3
V4
I1
I4

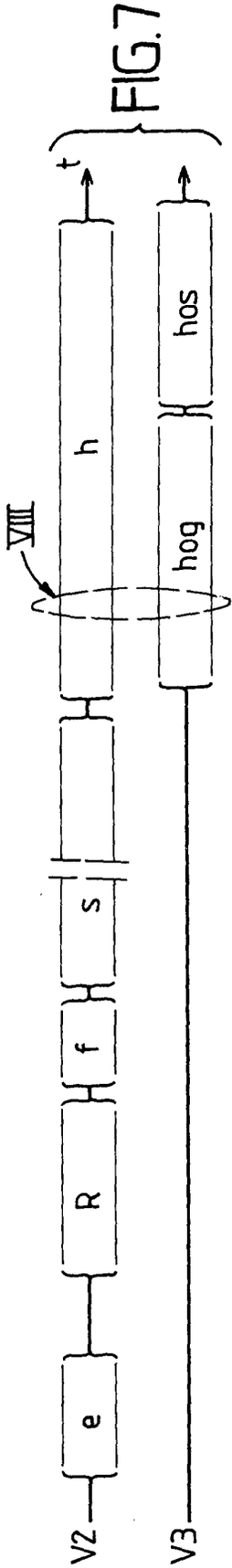
VIII
h
hos
hog
s
f
R
e
V2
V3
t

FIG.7

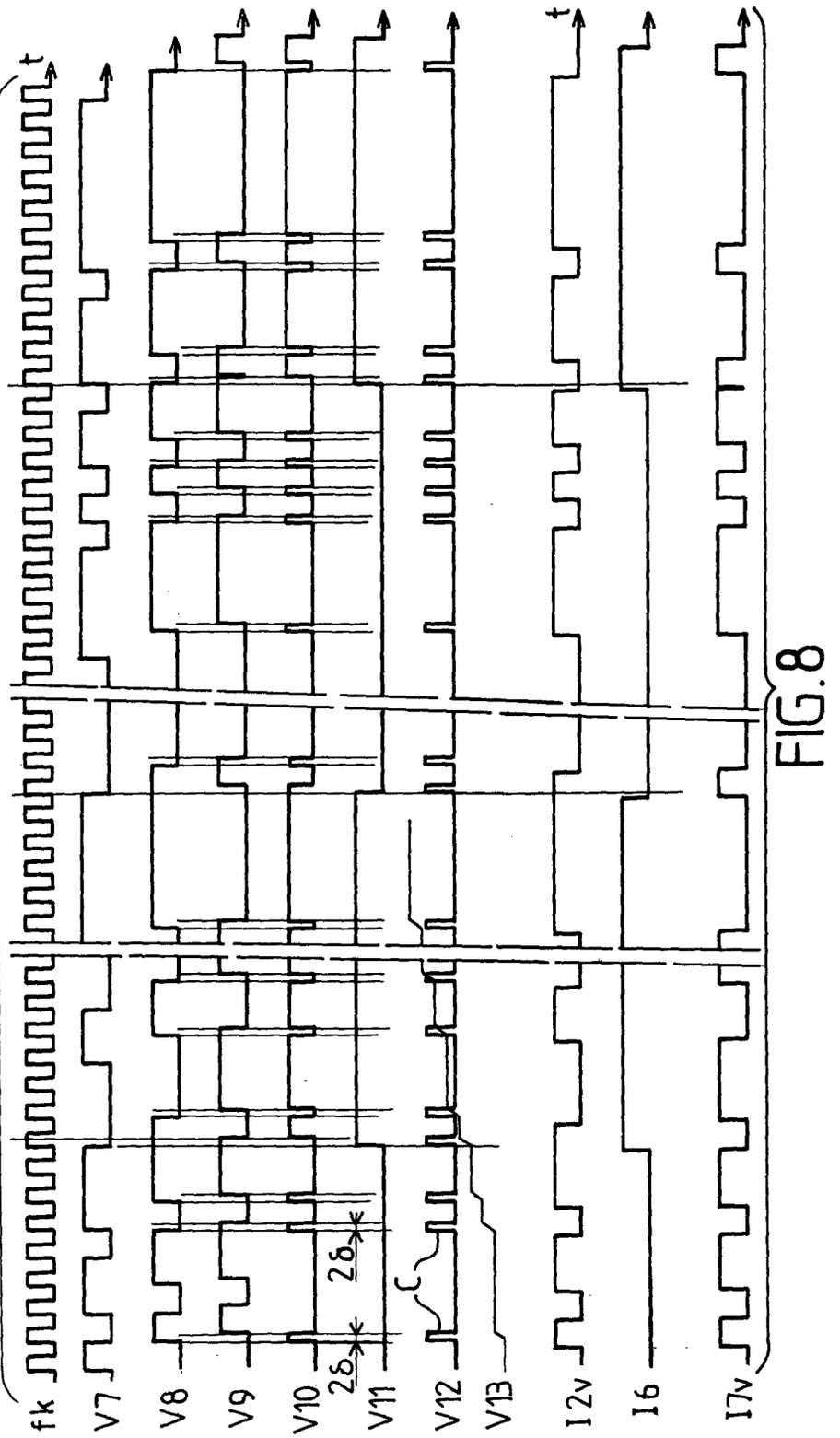
t
fk
V7
V8
V9
V10
V11
V12
V13
I2v
I6
I7v
2δ
2δ
C

FIG.8