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

(11) EP 1 061 211 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
20.12.2000 Bulletin 2000/51

(51) Int Cl.[7]: **E05B 49/00**, G07C 9/00

(21) Numéro de dépôt: **00401666.3**

(22) Date de dépôt: **13.06.2000**

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

(30) Priorité: **15.06.1999 FR 9907529**

(71) Demandeur: **Valeo Securité Habitacle**
94042 Créteil (FR)

(72) Inventeur: **Avenel, Jean-Jacques**
94430 Chennevieres (FR)

(74) Mandataire: **Lenne, Laurence**
Valeo Securité Habitacle
42, rue le Corbusier
Europarc
94042 Creteil (FR)

(54) Procédé pour sécuriser une transmission bidirectionnelle de données avec un identifiant et système pour sa mise en oeuvre

(57) L'invention concerne un procédé pour sécuriser une transmission bidirectionnelle de données, pour l'accès à un espace clos, en particulier à un véhicule automobile, consistant à établir un échange à distance de données entre un dispositif d'identification installé dans l'espace clos et un identifiant destiné à être porté par l'utilisateur, lorsque la distance entre l'identifiant et le dispositif d'identification est inférieure à une limite prédéterminée, l'accès n'étant autorisé lorsque le dispositif d'identification a authentifié l'identifiant, l'opération d'identification comprenant l'émission par le dispositif d'identification d'un premier signal codé d'identification et d'au moins un deuxième signal d'interrogation.

Pour empêcher un échange de données d'identification entre le dispositif d'identification et un répéteur non autorisé, sans passer par l'identifiant, le procédé consiste d'une part à décoder au niveau de l'identifiant, le premier signal codé d'identification reçu par l'identifiant en provenance du dispositif d'identification, au début de l'opération d'identification, à séquentiellement inverser la phase du deuxième signal d'interrogation reçu par l'identifiant en provenance du dispositif d'identification, en fonction du code d'identification préalablement obtenu par décodage, à réémettre ledit deuxième signal vers le dispositif d'identification afin que ce dernier puisse détecter le déphasage.

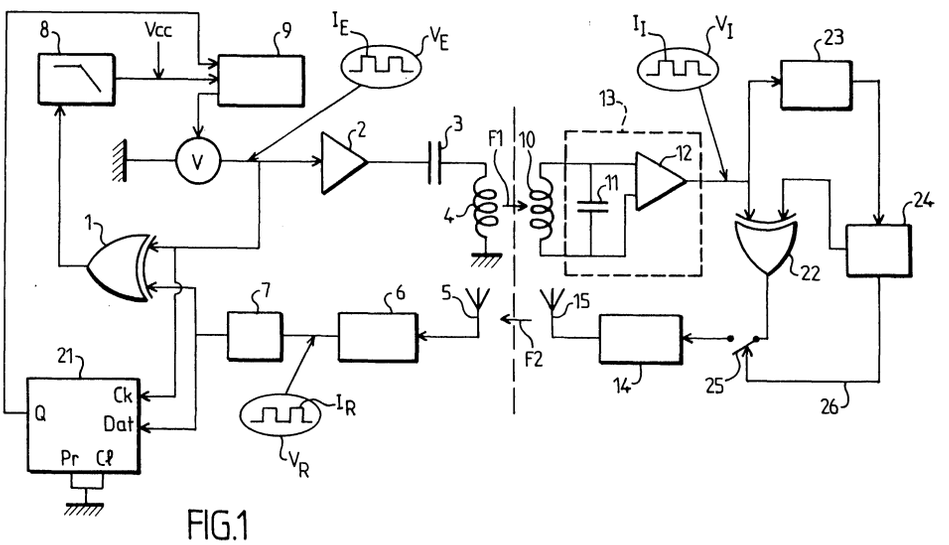

FIG.1

EP 1 061 211 A1

Description

[0001] L'invention est relative à un procédé pour sécuriser une transmission bidirectionnelle de données avec un identifiant et un système pour sa mise en oeuvre.

[0002] Un système de ce genre comprend généralement un dispositif d'identification ayant un circuit d'émission et un circuit de réception, installé dans l'espace clos, et un identifiant porté par un utilisateur qui souhaite obtenir l'accès, un échange de données entre dispositif d'identification et identifiant étant prévu pour s'établir normalement lorsque la distance entre l'identifiant et le dispositif d'identification est inférieure à une limite prédéterminée, l'accès n'étant autorisé que lorsque le dispositif d'identification a authentifié l'identifiant.

[0003] L'invention concerne plus particulièrement, parce que c'est dans ce cas que son application semble devoir présenter le plus d'intérêt, mais non exclusivement, un système pour sécuriser l'accès à un véhicule automobile dont les ouvrants, en particulier les portières de l'habitacle, comportent des serrures commandées par le système d'accès.

[0004] Dans ce type de système, l'utilisateur, pour obtenir l'accès, doit tout d'abord faire débuter une opération d'identification. Ce démarrage de l'opération peut être obtenu, par exemple, par action sur un bouton de commande situé sur l'ouvrant, ou par une commande à distance, ou éventuellement par un détecteur de présence installé dans l'espace clos. D'une manière générale, ce démarrage de l'opération d'identification est prévu pour nécessiter la proximité de l'utilisateur relativement à l'espace clos où il souhaite accéder.

[0005] L'opération d'identification s'effectue sur la base d'un échange de données entre le dispositif d'identification et l'identifiant constitué, par exemple, par un badge avec transpondeur électromagnétique. Suite au déclenchement de l'opération, le dispositif d'identification, installé dans l'espace clos, émet en général un signal d'interrogation qui active l'identifiant, lequel renvoie un signal codé analysé par le dispositif d'identification. Si le signal codé correspond au code autorisé, le dispositif d'identification autorise l'accès, par exemple en déverrouillant une ou des serrures. Les signaux échangés sont généralement des signaux électromagnétiques.

[0006] Pour renforcer la sécurité, le système est conçu de telle sorte que la portée de transmission soit réduite et qu'un échange de données d'identification entre dispositif d'identification et identifiant ne peut normalement s'établir que lorsque la distance entre l'espace clos et l'identifiant est inférieure à une limite prédéterminée, par exemple de l'ordre de quelques mètres.

[0007] Malgré ces précautions, un tel système d'accès court le risque d'être piraté par un autre ensemble d'émission-réception intercalé dans la liaison entre le dispositif d'identification et l'identifiant, cet autre ensemble d'émission-réception servant en fait uniquement de répéteur.

[0008] Par exemple, deux malfaiteurs agissant de conserve pourraient obtenir l'accès à l'espace clos de la manière suivante. Un premier malfaiteur, équipé d'un système d'émission-réception installé par exemple dans une sacoche, s'approche du véhicule fermé que vient de quitter un utilisateur autorisé, tandis qu'un second malfaiteur, équipé d'un système d'émission-réception semblable à celui du premier malfaiteur, suit l'utilisateur autorisé portant l'identifiant. Lorsque l'utilisateur autorisé est suffisamment éloigné, le premier malfaiteur déclenche une opération d'identification, par exemple par appui sur un bouton de commande situé sur un ouvrant. Les signaux émis par le dispositif d'identification sont relayés par le système d'émission-réception du premier malfaiteur vers le système du second malfaiteur, qui répète les signaux du dispositif d'identification vers l'identifiant. Ce dernier va alors répondre par le code autorisé, qui est retransmis par le système répéteur jusqu'au dispositif d'identification qui commande le déverrouillage des serrures et donne accès au malfaiteur.

[0009] Pour éviter un tel piratage, le principe consiste à détecter un temps de retard anormal, résultant de l'interposition d'un répéteur non autorisé entre le dispositif d'identification embarqué sur le véhicule et l'identifiant porté par l'utilisateur. Toutefois, si pour cette mesure de temps de retard anormal, le signal d'interrogation émis par le dispositif d'identification est simplement réémis, sans modulation, par l'identifiant en retour vers le véhicule, il est possible à un pirate de déterminer le moment où cette mesure du temps de retard anormal est effectuée et de renvoyer directement au véhicule le signal d'anti-piratage à l'aide uniquement du système d'émission/réception situé à proximité du véhicule. Autrement dit, le pirate peut court-circuiter la communication avec le véhicule, à l'aide d'un simple répéteur, sans passer par l'identifiant.

[0010] L'invention a pour but de proposer un procédé qui permet de sécuriser une transmission bidirectionnelle de données pour l'accès à un espace clos, en empêchant une éventuelle violation par un ensemble pirate d'émission-réception tel que celui évoqué ci-dessus.

[0011] Le principe de l'invention consiste, par exemple lors de la mesure d'un temps de retard, à ne pas utiliser l'identifiant en simple répéteur du signal émis par le véhicule, afin d'obliger le pirate à retransmettre le signal émis par l'identifiant, ce qui engendre nécessairement un temps de retard plus long.

[0012] A cet effet, l'invention a pour objet un procédé pour sécuriser une transmission bidirectionnelle de données, pour l'accès à un espace clos, en particulier à un véhicule automobile, consistant à établir un échange à distance de données entre un dispositif d'identification installé dans l'espace clos et un identifiant destiné à être porté par l'utilisateur, lorsque la distance entre l'identifiant et le dispositif d'identification est inférieure à une limite prédéterminée, l'accès n'étant autorisé que lorsque le dispositif d'identification a authentifié l'identifiant,

l'opération d'identification comprenant l'émission par le dispositif d'identification d'un premier signal codé d'identification et d'au moins un deuxième signal d'interrogation, caractérisé par le fait que, pour empêcher un échange de données d'identification entre le dispositif d'identification et un répéteur non autorisé, sans passer par l'identifiant, le procédé consiste, d'une part, à décoder, au niveau de l'identifiant, le premier signal codé d'identification reçu par l'identifiant en provenance du dispositif d'identification, au début de l'opération d'identification, à séquentiellement inverser la phase du deuxième signal d'interrogation reçu par l'identifiant en provenance du dispositif d'identification, en fonction du code d'identification préalablement obtenu par décodage, à réémettre ledit deuxième signal vers le dispositif d'identification, afin que ce dernier puisse détecter le déphasage entre le deuxième signal d'interrogation engendré par le dispositif d'identification et le deuxième signal reçu par le dispositif d'identification, en provenance de l'identifiant, et à maintenir l'interdiction d'accès lorsque la séquence de déphasage détectée ne correspond pas au code d'identification connu par le dispositif d'identification. Ce code d'identification peut être constitué d'une séquence pseudo-aléatoire selon un algorithme prédéterminé, que le pirate ne peut pas connaître. Ainsi, si le pirate utilise un simple répéteur pour dialoguer directement avec le dispositif d'identification, ce dernier recevra le deuxième signal d'interrogation, sans inversion de phase, ce qui ne correspondra pas au code d'identification connu par le dispositif d'identification, empêchant ainsi l'accès au véhicule.

[0013] Avantageusement, le deuxième signal d'interrogation engendré par le dispositif d'identification est un signal oscillant pulsé et le code d'identification est un code numérique à plusieurs bits, par exemple à trois octets, de façon à successivement activer ou désactiver l'inversion de phase d'une impulsion du deuxième signal d'interrogation, au niveau de l'identifiant, selon la valeur binaire de chaque bit de ce code d'identification.

[0014] Selon une autre caractéristique, le procédé consiste, au niveau du dispositif d'identification, à ajouter un déphasage supplémentaire de 90° au deuxième signal d'interrogation reçu par le dispositif d'identification, et, à l'étape de détection de déphasage, à affecter une valeur binaire pour chaque impulsion du deuxième signal, selon que la phase du deuxième signal reçu est en avance ou en retard d'environ 90° par rapport à la phase du deuxième signal engendré, afin de vérifier si la séquence de valeurs binaires ainsi affectées correspond bien au code d'identification connu par le dispositif d'identification.

[0015] Dans une forme de réalisation préférée, pour empêcher un échange de données d'identification à une distance supérieure à la limite prédéterminée précitée, en particulier par interposition d'un répéteur non autorisé entre le dispositif d'identification et l'identifiant, le procédé consiste, en outre, au niveau du dispositif d'identification, à discriminer la phase entre le deuxième signal d'interrogation engendré par le dispositif d'identification et ledit deuxième signal reçu par le dispositif d'identification en provenance de l'identifiant, à filtrer le signal résultant de la discrimination de phase pour délivrer un signal continu représentatif du déphasage et à maintenir l'interdiction d'accès lorsque la différence entre l'amplitude dudit signal continu et l'amplitude d'un signal de référence dépasse une valeur de seuil prédéterminée.

[0016] L'invention vise également un système pour la mise en oeuvre du procédé précité, dans lequel le dispositif d'identification comprend un circuit d'émission et un circuit de réception, et l'identifiant comporte un émetteur et un récepteur, caractérisé par le fait qu'il comporte, au niveau de l'identifiant, un moyen de décodage pour décoder le premier signal codé d'identification, un moyen inverseur de phase pour inverser la phase d'au moins un deuxième signal d'interrogation selon une séquence commandée par une unité centrale de commande en fonction du code d'identification fourni par le moyen de décodage, et au niveau du dispositif d'identification, un moyen détecteur de déphasage recevant, en entrée, à la fois le deuxième signal d'interrogation engendré par un générateur du dispositif d'identification, et ledit deuxième signal d'interrogation reçu par le circuit de réception du dispositif d'identification en provenance de l'identifiant, et une unité centrale de traitement apte à analyser le déphasage ainsi détecté en fonction du code d'identification connu par le dispositif d'identification.

[0017] Avantageusement, le générateur du dispositif d'identification engendre le deuxième signal d'interrogation sous la forme d'un signal oscillant pulsé, dont chaque impulsion a une fréquence porteuse prédéterminée, par exemple en basse fréquence à 125 KHz, lesdites impulsions ayant une période de récurrence prédéterminée, par exemple de l'ordre de 8 µs, et le code d'identification est un code binaire à plusieurs bits, de durée unitaire par exemple de 200 µs, par exemple à trois octets, la valeur 1 ou 0 de chaque bit étant destinée à activer ou désactiver le moyen inverseur de phase pendant une durée correspondant sensiblement à celle du bit 1 ou 0.

[0018] Dans une forme de réalisation particulière, l'identifiant comporte un récepteur basse fréquence ayant un circuit de remise en forme du signal dont la sortie est reliée, d'une part, au moyen de décodage précité, et d'autre part, à une entrée d'une porte logique OU exclusif qui constitue le moyen inverseur de phase précitée, l'autre entrée de ladite porte recevant les bits du code d'identification selon la fréquence de récurrence des impulsions du deuxième signal d'interrogation, la sortie de ladite porte logique étant reliée à un émetteur radio-fréquence modulé par ledit signal de sortie de la porte logique.

[0019] Dans ce cas, un interrupteur peut être intercalé entre ladite porte logique et l'émetteur radio-fréquence de l'identifiant, ledit interrupteur étant commandé par

l'unité centrale de commande pour ouvrir la liaison entre la porte logique et l'émetteur pendant la phase de décodage du premier signal d'identification et pour fermer ladite liaison pendant la réception et la réémission du deuxième signal d'interrogation par l'identifiant.

[0020] On peut également prévoir qu'un moyen de déphasage est intercalé entre un récepteur radio-fréquence du dispositif d'identification et le moyen de détection de déphasage précité, pour ajouter au deuxième signal d'interrogation reçu en provenance de l'identifiant un déphasage supplémentaire de 90° à l'entrée dudit moyen de détection de déphasage, ce dernier étant constitué d'une bascule D recevant sur une autre entrée le deuxième signal d'interrogation engendré par le générateur du dispositif d'identification, pour délivrer en sortie, pour chaque impulsion dudit deuxième signal d'interrogation, une valeur binaire 1 ou 0 selon que la phase du deuxième signal d'interrogation reçu est en avance ou en retard d'environ 90° par rapport à la phase du deuxième signal d'interrogation engendré, la sortie de ladite bascule D étant reliée à l'unité centrale de traitement pour la comparer au code d'identification précité.

[0021] Avantageusement, pour empêcher un échange de données d'identification à une distance supérieure à la limite prédéterminée, en particulier par interposition d'un répéteur non autorisé entre le dispositif d'identification et l'identifiant, le système comprend, en parallèle au moyen de détection de déphasage, un moyen discriminateur de phase recevant, en entrée, le deuxième signal engendré par le générateur du dispositif d'identification et le deuxième signal reçu par le circuit de réception en provenance de l'identifiant, un moyen de filtrage étant connecté en sortie dudit moyen discriminateur de phase, pour délivrer, en sortie, un signal continu représentatif du déphasage des signaux précités, ledit signal continu étant délivré à l'unité centrale de traitement qui est sensible à la différence entre l'amplitude dudit signal continu délivré et l'amplitude d'un signal de référence, pour maintenir l'interdiction d'accès lorsque ladite différence dépasse une valeur de seuil prédéterminée.

[0022] Dans ce cas, on peut prévoir que le circuit de réception du dispositif d'identification comporte une antenne reliée à un récepteur radio-fréquence, par exemple à 434 MHz, connecté, d'une part, à une entrée du moyen discriminateur de phase précité et, d'autre part, à une entrée du moyen de détection de phase précité, et le circuit d'émission du dispositif d'identification comporte un générateur basse fréquence, par exemple à 125 KHz connecté, en parallèle, à l'autre entrée du moyen discriminateur de phase, à l'autre entrée du moyen détecteur de déphasage, et à un amplificateur d'antenne.

[0023] Selon une forme de réalisation particulière, le moyen discriminateur de phase précité est une porte logique OU exclusif qui délivre en sortie un signal dont la composante continue varie linéairement en fonction du déphasage entre les deuxièmes signaux engendré et reçu précités sur une demi-période. Dans ce cas, le moyen de filtrage précité peut être un filtre passe-bas par exemple avec une fréquence de coupure de l'ordre de 10 KHz.

[0024] Avantageusement, l'unité centrale de traitement comporte un micro-contrôleur équipé d'un convertisseur analogique/numérique, pour traiter numériquement la différence de valeur entre la tension continue délivrée et la tension de référence, et pour comparer les valeurs binaires du signal de sortie de la bascule D et le code d'identification.

[0025] Dans ce cas, le générateur basse-fréquence du dispositif d'identification peut être modulé en fréquence par l'unité centrale de traitement, de préférence de manière aléatoire, par exemple sur une plage de 120 à 130 KHz et avec une période d'environ une ms.

[0026] Selon une autre caractéristique, le système comporte un moyen de mesure du temps de retard entre les deuxièmes signaux engendré et reçu précités, afin que l'unité centrale de traitement maintienne l'interdiction d'accès lorsque la valeur du temps de retard mesurée dépasse une valeur de seuil prédéterminée, par exemple une ou deux périodes de récurrence dudit deuxième signal.

[0027] De préférence, la tension de référence, à laquelle est comparée la tension continue délivrée par le moyen de filtrage, est constituée par une valeur initialement mémorisée, qui est apprise par le système.

[0028] Pour mieux faire comprendre l'objet de l'invention, on va en décrire maintenant, à titre d'exemple purement illustratif et non limitatif, un mode de réalisation représenté sur le dessin annexé.

[0029] Sur ce dessin :

- la figure 1 est un schéma synoptique fonctionnel du système selon l'invention ; et
- la figure 2 est un graphique représentant la valeur de la tension continue en fonction du déphasage.

[0030] Sur la figure 1, le dispositif d'identification embarqué par exemple sur un véhicule, comporte un générateur de tension V basse fréquence BF, par exemple à 125 KHz, délivrant en sortie une tension V_E sous forme de créneaux. La tension V_E est envoyée, d'une part, à une entrée d'une porte logique OU exclusif 1 et à une entrée Ck d'une bascule 21 dite bascule D, et d'autre part, à l'entrée d'un amplificateur 2. La sortie de l'amplificateur 2 est reliée à une capacité 3 et à une inductance 4 en série, une borne de l'inductance 4 étant reliée à la masse. L'inductance 4 constitue l'antenne d'émission BF du dispositif d'identification.

[0031] Le dispositif d'identification comporte, en outre, une antenne 5 reliée à l'entrée d'un récepteur 6 radio fréquence RF, par exemple à 434 MHz. La sortie du récepteur RF 6 est reliée en série à un moyen de déphasage 7 pour introduire un déphasage de 90° dans le signal reçu V_R. La sortie du moyen de déphasage 7 est reliée en parallèle à l'autre entrée de la porte logique

1 et à une autre entrée Dat de la bascule D.

[0032] La porte logique 1 est reliée en sortie à un filtre passe-bas 8 d'ordre quatre, avec une fréquence de coupure d'environ 10 KHz. Le filtre 8 permet de délivrer en sortie la composante continue Vcc du signal sortant de la porte logique 1. La tension Vcc est reçue par une unité de traitement 9 comportant un micro-contrôleur équipé d'un convertisseur analogique/numérique à 8 bits. L'unité de traitement 9 est apte à commander le générateur BF précité, dont une borne est reliée à la masse.

[0033] Les bornes Pr et Cℓ de la bascule D sont reliées à la masse et la sortie Q de la bascule 21 est reliée à l'unité 9. La bascule 21 ne sera pas décrite plus en détail, car elle est connue en soi.

[0034] L'identifiant, porté par exemple sur un badge, comporte une inductance 10 qui est branchée en parallèle sur une capacité 11 et aux deux bornes d'entrée d'un comparateur 12. L'ensemble 11, 12 constitue un récepteur BF 13 comportant un circuit de réveil à très faible consommation qui effectue une remise en forme du signal pour délivrer un signal induit V_I sous forme de créneaux. La sortie du comparateur 12 est reliée, d'une part, à une entrée d'une autre porte logique OU exclusif 22 et à l'entrée d'un moyen de décodage 23. La sortie du moyen de décodage est reliée à une unité centrale de commande 24 qui est apte à commander un interrupteur 25 par une liaison 26 et apte à fournir un signal constitué d'une séquence de valeurs binaires à une deuxième entrée de la porte logique 22. Le signal de sortie de la porte 22 permet de moduler un émetteur RF 14 qui délivre un signal modulé vers une antenne 15 de l'identifiant, lorsque l'interrupteur 25 est fermé.

[0035] La flèche F1 indique la transmission du signal BF entre l'antenne 4 et l'antenne 10, et la flèche F2 indique la transmission du signal RF entre l'antenne 15 et l'antenne 5.

[0036] On va maintenant décrire un premier exemple de fonctionnement du système de l'invention.

[0037] Le générateur V engendre un premier signal codé d'identification, composé de bits d'identification, qui est émis par l'antenne 4 du dispositif d'identification et reçu par l'antenne 10 de l'identifiant. Ce premier signal code d'identification est décodé par le moyen de décodage 23 qui, simultanément, donne l'ordre à l'unité centrale de commande 24 de commander l'ouverture de l'interrupteur 25, pour éviter une réémission de ce premier signal par l'identifiant. Le premier signal codé d'identification est émis avec une période d'environ 200 µs par bit d'identification.

[0038] Puis, le générateur V engendre un deuxième signal d'interrogation qui est constitué d'une tension V_E sous forme de créneaux avec une fréquence porteuse de 125 KHz et une amplitude de crête, pour chaque impulsion I_E, de 5 Volts. Dans ce cas, la période de récurrence des impulsions du deuxième signal est de 8 µs. Ce deuxième signal d'interrogation est reçu par l'identifiant et délivre en sortie de son récepteur 13 un signal oscillant en créneaux V_I dont l'enveloppe du signal est représentée sur la figure 1. Le signal V_I est reçu à l'entrée de la porte logique 22 qui reçoit, en outre, en entrée un signal continu sous forme de créneaux représentatifs des bits successifs du code d'identification préalablement obtenu par l'intermédiaire du moyen de décodage 23. Dans ce cas, l'unité centrale de commande 24 a commandé l'interrupteur 25 pour fermer la liaison vers l'émetteur 14. Si un bit du code d'identification est à 0, lors d'une impulsion I_I du signal V_I, la porte logique 22 délivrera en sortie ladite impulsion I_I, alors que si le bit est à 1, la porte logique 22 sortira une impulsion dont la phase sera inversée de 180° et ce pendant toute la durée d'un bit d'identification, soit 200 µs.

[0039] Bien entendu, le deuxième signal d'interrogation ne passe pas par le moyen de décodage 23.

[0040] Le signal reçu V_R présente un léger déphasage par rapport au signal V_E, par exemple de l'ordre de quelques centaines de ns, du fait du temps de transmission du signal résultant de la distance et des composants électroniques.

[0041] Dans le cas où le moyen de déphasage 7 est absent, la porte logique 1 délivrera en sortie un signal dont la fréquence sera double, c'est-à-dire de l'ordre de 250 KHz. Le filtre passe-bas 8 permettra d'éliminer la fréquence porteuse à 250 KHz, pour ne garder que la composante continue du signal.

[0042] Si les deux antennes 4, 10 sont positionnées de manière à être en phase (c'est-à-dire, avec $\Delta\varphi = 0$), la tension Vcc sera de l'ordre de 0 V, comme indiqué sur le graphique de la figure 2. Si l'on tient compte du léger retard introduit par la transmission bidirectionnelle des données F1 et F2, qui est de l'ordre de quelques centaines de ns, la tension résultante Vcc sera en fait de l'ordre de quelques centaines de mV. En effet, la porte logique 1 délivre un signal dont la composante continue varie entre 0 et 5 V, pour un déphasage $\Delta\varphi$ compris entre 0 et 180°, comme visible sur la figure 2. On peut ainsi détecter un déphasage avec une précision de l'ordre de 5 V/180° = 28 mV/°. Etant donné que, pour le signal V_E, la période de 8 µs correspond à 360°, un retard de l'ordre de 100 ns, qui correspond à 0,1 µs, se traduit par un déphasage de 0,1 x 360/8 = 4,5°. Ainsi, un léger retard de l'ordre de 100 ns correspond à une tension continue Vcc égale à 4,5° x 28 mV/° = 125 mV.

[0043] A titre d'exemple, la valeur de seuil prédéterminée pourrait être de l'ordre de 250 mV, ce qui correspondrait à un retard d'environ 200 ns, alors que la valeur de la tension de référence serait de 0 V.

[0044] En revanche, si les deux bobines 4, 10 sont en opposition de phase, c'est-à-dire avec un déphasage $\Delta\varphi$ = 180°, la valeur de la tension continue Vcc sera de 5 V, comme visible sur la figure 2.

[0045] Par conséquent, si Vcc est par exemple compris entre 0,25 et 4,75 V, cela signifiera que les signaux émis et reçu sont déphasés d'une manière irrégulière, ce qui maintiendra l'interdiction d'accès au véhicule et/ou pourra déclencher une alarme sonore ou visuelle.

[0046] Dans le cas où le moyen de déphasage 7 est

absent, on n'utilise pas la bascule 21, mais on utilise uniquement la porte logique 1, en tant que moyen détecteur de déphasage. Ainsi, pour chaque impulsion I_R du signal reçu V_R , si Vcc est entre 0 et 1 volt, l'unité centrale de traitement 9 pourra affecter à ladite impulsion une valeur binaire égale à 0, et si la tension Vcc est comprise entre 4 et 5 volts, on peut affecter à l'impulsion une valeur binaire égale à 1, afin de comparer la séquence desdites valeurs binaires au code d'identification connu par le véhicule. Ainsi, la porte logique 1 peut servir à la fois pour détecter un retard et pour vérifier que le signal est bien passé par l'identifiant.

[0047] Bien entendu, l'invention suppose que l'antenne de réception de l'identifiant ne soit pas retournée par rapport à l'antenne émettrice du dispositif d'identification, pendant l'analyse du second signal sinon la comparaison avec le code d'identification sera faussée.

[0048] Toutefois, pour éviter d'avoir deux valeurs possibles de tension de référence, à savoir 0 V et 5 V, selon que les bobines BF sont en phase ou en opposition de phase, on peut ajouter le moyen de déphasage 7 pour introduire un déphasage supplémentaire de 90°. Ainsi, que les bobines 4, 10 soient en phase ou en opposition de phase, la porte logique 1 détectera un déphasage qui sera toujours de l'ordre de 90°, ce qui correspond à un signal Vcc de l'ordre de 2,5 V, avec une marge d'erreur de l'ordre de 10 %, c'est-à-dire 0,25 V. Le fait d'ajouter le moyen de déphasage 7 permet d'avoir en mémoire une seule valeur de tension de référence.

[0049] Ainsi, si un pirate introduit un répéteur entre le dispositif d'identification et l'identifiant, le temps de retard global pourrait, par exemple, être de l'ordre de 1 µs, ce qui correspondrait à un déphasage de 45° supplémentaires entre le signal reçu et le signal émis. La tension continue résultante Vcc varierait alors de 45° x 28 mV/° = 1,25 V, ce qui est bien supérieur à la valeur de seuil de 250 mV.

[0050] Toutefois, si un pirate vient à connaître le système selon l'invention, il pourrait chercher à augmenter le déphasage, pour le porter, par exemple, de 45° à 180°, ce qui rendrait l'utilisation du répéteur transparent pour le système. Autrement dit, le pirate pourrait, de manière artificielle, augmenter le temps de retard du signal reçu, de façon que le signal reçu soit toujours en phase ou en opposition de phase avec le signal émis.

[0051] Pour éviter cet inconvénient, il suffit de faire varier, de manière aléatoire, la fréquence du signal engendré, par exemple sur une plage allant de 120 à 130 KHz, avec une variation de la fréquence, par exemple toutes les millisecondes.

[0052] Par exemple, si le pirate pense que la fréquence d'émission est de 125 KHz, il pourra chercher à renvoyer le signal avec un temps de retard de l'ordre de 8 µs. Si, toutefois, le signal d'émission a en fait, à cet instant précis, une fréquence de 120 KHz, ce qui correspond à une période de 8,33 µs, le signal reçu sera déphasé par rapport au signal émis avec un temps de retard de 0,33 µs, ce qui correspondra à un déphasage d'environ 14° et donc à une variation de la tension continue Vc de l'ordre de 0,4 V, ce qui est bien supérieur à la valeur de seuil de 250 mV.

[0053] Si le pirate sait que la fréquence d'émission peut varier, il pourrait, tout d'abord, analyser le signal émis par le dispositif d'identification sur une période complète, afin d'identifier sa fréquence, puis renvoyer le signal vers le dispositif d'identification, avec un retard global de deux ou plus périodes, ce qui rendrait à nouveau le piratage transparent vis-à-vis du système.

[0054] Pour éviter ce cas, il suffirait alors de rajouter un moyen de mesure du temps de retard entre le signal émis et le signal reçu. En effet, dès lors qu'il sera nécessaire au pirate de mesurer d'abord la fréquence du signal émis sur une période, puis de le renvoyer après au moins deux périodes, le temps de retard résultant sera suffisamment grand pour pouvoir être détecté par un moyen de mesure de temps de retard suffisamment simple et économique.

[0055] Dans le cas où le moyen de déphasage 7 est utilisé, on peut utiliser la bascule 21 précitée, pour détecter le déphasage entre les signaux sur ses entrées Ck et Dat, de façon que sa sortie Q délivre un signal binaire dont la valeur est égale à 1, si l'entrée Ck est en retard de 90° par rapport à l'entrée Dat et égale à 0 si l'entrée Ck est en avance de 90° par rapport à l'entrée Dat. La sortie Q de la bascule 21 est analysée par le microprocesseur de l'unité centrale 9, afin de la comparer au code d'identification connu par le dispositif connu d'identification.

[0056] Enfin, il est à noter que si l'on utilise un convertisseur analogique/numérique à 8 bits, on pourra obtenir une numérisation du signal Vcc avec une précision de 5 V/256, c'est-à-dire environ 19,5 mV/bit. Etant donné que la porte logique 1 permettait d'avoir une précision de 27 mV/°, on obtient avec le convertisseur analogique/numérique une précision supérieure à 1° par bit.

[0057] Bien que l'invention ait été décrite en liaison avec plusieurs exemples de réalisation particuliers, il est bien évident qu'elle n'y ait 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. Procédé pour sécuriser une transmission bidirectionnelle de données, pour l'accès à un espace clos, en particulier à un véhicule automobile, consistant à établir un échange à distance de données entre un dispositif d'identification installé dans l'espace clos et un identifiant destiné à être porté par l'utilisateur, lorsque la distance entre l'identifiant et le dispositif d'identification est inférieure à une limite prédéterminée, l'accès n'étant autorisé que lorsque le dispositif d'identification a authentifié l'identifiant, l'opération d'identification comprenant l'émission

par le dispositif d'identification d'un premier signal codé d'identification et d'au moins un deuxième signal d'interrogation (V_E), caractérisé par le fait que, pour empêcher un échange de données d'identification entre le dispositif d'identification et un répéteur non autorisé, sans passer par l'identifiant, le procédé consiste, d'une part, à décoder, au niveau de l'identifiant, le premier signal codé d'identification reçu par l'identifiant en provenance du dispositif d'identification, au début de l'opération d'identification, à séquentiellement inverser la phase du deuxième signal d'interrogation reçu par l'identifiant en provenance du dispositif d'identification, en fonction du code d'identification préalablement obtenu par décodage, à réémettre ledit deuxième signal vers le dispositif d'identification, afin que ce dernier puisse détecter le déphasage entre le deuxième signal d'interrogation (V_E) engendré par le dispositif d'identification et le deuxième signal (V_R) reçu par le dispositif d'identification, en provenance de l'identifiant, et à maintenir l'interdiction d'accès lorsque la séquence de déphasage détectée ne correspond pas au code d'identification connu par le dispositif d'identification.

2. Procédé selon la revendication 1, caractérisé par le fait que le deuxième signal d'interrogation (V_E) engendré par le dispositif d'identification est un signal oscillant pulsé et le code d'identification est un code numérique à plusieurs bits, par exemple à trois octets, de façon à successivement activer ou désactiver l'inversion de phase d'une impulsion (I_I) du deuxième signal d'interrogation (V_I), au niveau de l'identifiant, selon la valeur binaire de chaque bit de ce code d'identification.

3. Procédé selon la revendication 2, caractérisé par le fait qu'il consiste, au niveau du dispositif d'identification, à ajouter un déphasage supplémentaire de 90° au deuxième signal d'interrogation (V_R) reçu par le dispositif d'identification, et, à l'étape de détection de déphasage, à affecter une valeur binaire pour chaque impulsion du deuxième signal, selon que la phase du deuxième signal reçu est en avance ou en retard d'environ 90° par rapport à la phase du deuxième signal engendré (V_E), afin de vérifier si la séquence de valeurs binaires ainsi affectées correspond bien au code d'identification connu par le dispositif d'identification.

4. Procédé selon l'une des revendications 1 à 3, caractérisé par le fait que, pour empêcher un échange de données d'identification à une distance supérieure à la limite prédéterminée précitée, en particulier par interposition d'un répéteur non autorisé entre le dispositif d'identification et l'identifiant, le procédé consiste, en outre, au niveau du dispositif d'identification, à discriminer la phase entre le deuxième signal d'interrogation (V_E) engendré par le dispositif d'identification et ledit deuxième signal (V_R) reçu par le dispositif d'identification en provenance de l'identifiant, à filtrer le signal résultant de la discrimination de phase pour délivrer un signal continu représentatif du déphasage et à maintenir l'interdiction d'accès lorsque la différence entre l'amplitude dudit signal continu (Vcc) et l'amplitude d'un signal de référence dépasse une valeur de seuil prédéterminée.

5. Système pour la mise en oeuvre du procédé selon l'une des revendications 1 à 4, dans lequel le dispositif d'identification comprend un circuit d'émission (2-4) et un circuit de réception (5-7), et l'identifiant comporte un émetteur (14) et un récepteur (13), caractérisé par le fait qu'il comporte, au niveau de l'identifiant, un moyen de décodage (23) pour décoder le premier signal codé d'identification, un moyen inverseur de phase (22) pour inverser la phase d'au moins un deuxième signal d'interrogation (V_I) selon une séquence commandée par une unité centrale de commande (24) en fonction du code d'identification fourni par le moyen de décodage, et au niveau du dispositif d'identification, un moyen détecteur de déphasage (21) recevant, en entrée, à la fois le deuxième signal d'interrogation (V_E) engendré par un générateur (V) du dispositif d'identification, et ledit deuxième signal d'interrogation (V_R) reçu par le circuit de réception du dispositif d'identification en provenance de l'identifiant, et une unité centrale de traitement (9) apte à analyser le déphasage ainsi détecté en fonction du code d'identification connu par le dispositif d'identification.

6. Système selon la revendication 5, caractérisé par le fait que le générateur (V) du dispositif d'identification engendre le deuxième signal d'interrogation (V_E) sous la forme d'un signal oscillant pulsé, dont chaque impulsion (I_E) a une fréquence porteuse prédéterminée, par exemple en basse fréquence à 125 KHz, lesdites impulsions ayant une période de récurrence prédéterminée, par exemple de l'ordre de 8 µs, et le code d'identification est un code binaire à plusieurs bits, de durée unitaire par exemple de 200 µs, par exemple à trois octets, la valeur 1 ou 0 de chaque bit étant destinée à activer ou désactiver le moyen inverseur de phase (22) pendant une durée correspondant sensiblement à celle du bit 1 ou 0.

7. Système selon la revendication 6, caractérisé par le fait que l'identifiant comporte un récepteur basse fréquence (13) ayant un circuit de remise en forme du signal dont la sortie est reliée, d'une part, au moyen de décodage (23) précité, et d'autre part, à une entrée d'une porte logique OU exclusif (22) qui

constitue le moyen inverseur de phase précitée, l'autre entrée de ladite porte recevant les bits du code d'identification selon la fréquence de récurrence des impulsions (I_I) du deuxième signal d'interrogation (V_I), la sortie de ladite porte logique étant reliée à un émetteur radio-fréquence (14) modulé par ledit signal de sortie de la porte logique.

8. Système selon la revendication 7, caractérisé par le fait qu'un interrupteur est intercalé entre ladite porte logique (22) et l'émetteur radio-fréquence (14) de l'identifiant, ledit interrupteur étant commandé par l'unité centrale de commande (24) pour ouvrir la liaison entre la porte logique et l'émetteur pendant la phase de décodage du premier signal d'identification et pour fermer ladite liaison pendant la réception et la réémission du deuxième signal d'interrogation par l'identifiant.

9. Système selon l'une des revendications 5 à 8, caractérisé par le fait qu'un moyen de déphasage (7) est intercalé entre un récepteur radio-fréquence (6) du dispositif d'identification et le moyen de détection de déphasage (21) précité, pour ajouter au deuxième signal d'interrogation (V_R) reçu en provenance de l'identifiant un déphasage supplémentaire de 90° à l'entrée dudit moyen de détection de déphasage, ce dernier étant constitué d'une bascule D recevant sur une autre entrée le deuxième signal d'interrogation (V_E) engendré par le générateur (V) du dispositif d'identification, pour délivrer en sortie, pour chaque impulsion dudit deuxième signal d'interrogation, une valeur binaire 1 ou 0 selon que la phase du deuxième signal d'interrogation reçu (V_R) est en avance ou en retard d'environ 90° par rapport à la phase du deuxième signal d'interrogation engendré (V_E), la sortie de ladite bascule D étant reliée à l'unité centrale de traitement (9) pour la comparer au code d'identification précité.

10. Système selon l'une des revendications 5 à 9, caractérisé par le fait que, pour empêcher un échange de données d'identification à une distance supérieure à la limite prédéterminée, en particulier par interposition d'un répéteur non autorisé entre le dispositif d'identification et l'identifiant, le système comprend, en parallèle au moyen de détection de déphasage (21), un moyen discriminateur de phase (1) recevant, en entrée, le deuxième signal (V_E) engendré par le générateur (V) du dispositif d'identification et le deuxième signal (V_R) reçu par le circuit de réception (5-7) en provenance de l'identifiant, un moyen de filtrage (8) étant connecté en sortie dudit moyen discriminateur de phase, pour délivrer, en sortie, un signal continu (Vcc) représentatif du déphasage des signaux précités, ledit signal continu étant délivré à l'unité centrale de traitement (9) qui est sensible à la différence entre l'amplitude dudit signal continu délivré et l'amplitude d'un signal de référence, pour maintenir l'interdiction d'accès lorsque ladite différence dépasse une valeur de seuil prédéterminée.

11. Système selon la revendication 10, caractérisé par le fait que le circuit de réception (5-7) du dispositif d'identification comporte une antenne (5) reliée à un récepteur radio-fréquence (6), par exemple à 434 MHz, connecté, d'une part, à une entrée du moyen discriminateur de phase précité (1) et, d'autre part, à une entrée du moyen de détection de phase précité (21), et le circuit d'émission (2-4) du dispositif d'identification comporte un générateur basse fréquence (V), par exemple à 125 KHz connecté, en parallèle, à l'autre entrée du moyen discriminateur de phase, à l'autre entrée du moyen détecteur de déphasage, et à un amplificateur d'antenne (2).

12. Système selon la revendication 10 ou 11, caractérisé par le fait que le moyen discriminateur de phase précité (1) est une porte logique OU exclusif qui délivre en sortie un signal dont la composante continue varie linéairement en fonction du déphasage entre les deuxièmes signaux engendré (V_E) et reçu (V_R) précités sur une demi-période.

13. Système selon la revendication 12, caractérisé par le fait que le moyen de filtrage précité (8) est un filtre passe-bas par exemple avec une fréquence de coupure de l'ordre de 10 KHz.

14. Système selon l'une des revendications 10 à 13, caractérisé par le fait que l'unité centrale de traitement (9) comporte un micro-contrôleur équipé d'un convertisseur analogique/numérique, pour traiter numériquement la différence de valeur entre la tension continue délivrée (Vcc) et la tension de référence, et pour comparer les valeurs binaires du signal de sortie de la bascule D (21) et le code d'identification.

15. Système selon la revendication 14, caractérisé par le fait que le générateur basse-fréquence (V) du dispositif d'identification est modulé en fréquence par l'unité centrale de traitement (9), de préférence de manière aléatoire, par exemple sur une plage de 120 à 130 KHz et avec une période d'environ une ms.

16. Système selon l'une des revendications 10 à 15, caractérisé par le fait que le système comporte un moyen de mesure du temps de retard entre les deuxièmes signaux engendré et reçu précités, afin que l'unité centrale de traitement (9) maintienne l'interdiction d'accès lorsque la valeur du temps de retard mesurée dépasse une valeur de seuil prédéterminée, par exemple une ou deux périodes de ré-

currence dudit deuxième signal.

17. Système selon l'une des revendications 10 à 17, caractérisé par le fait que la tension de référence, à laquelle est comparée la tension continue délivrée (Vcc) par le moyen de filtrage (8), est constituée par une valeur initialement mémorisée, qui est apprise par le système.

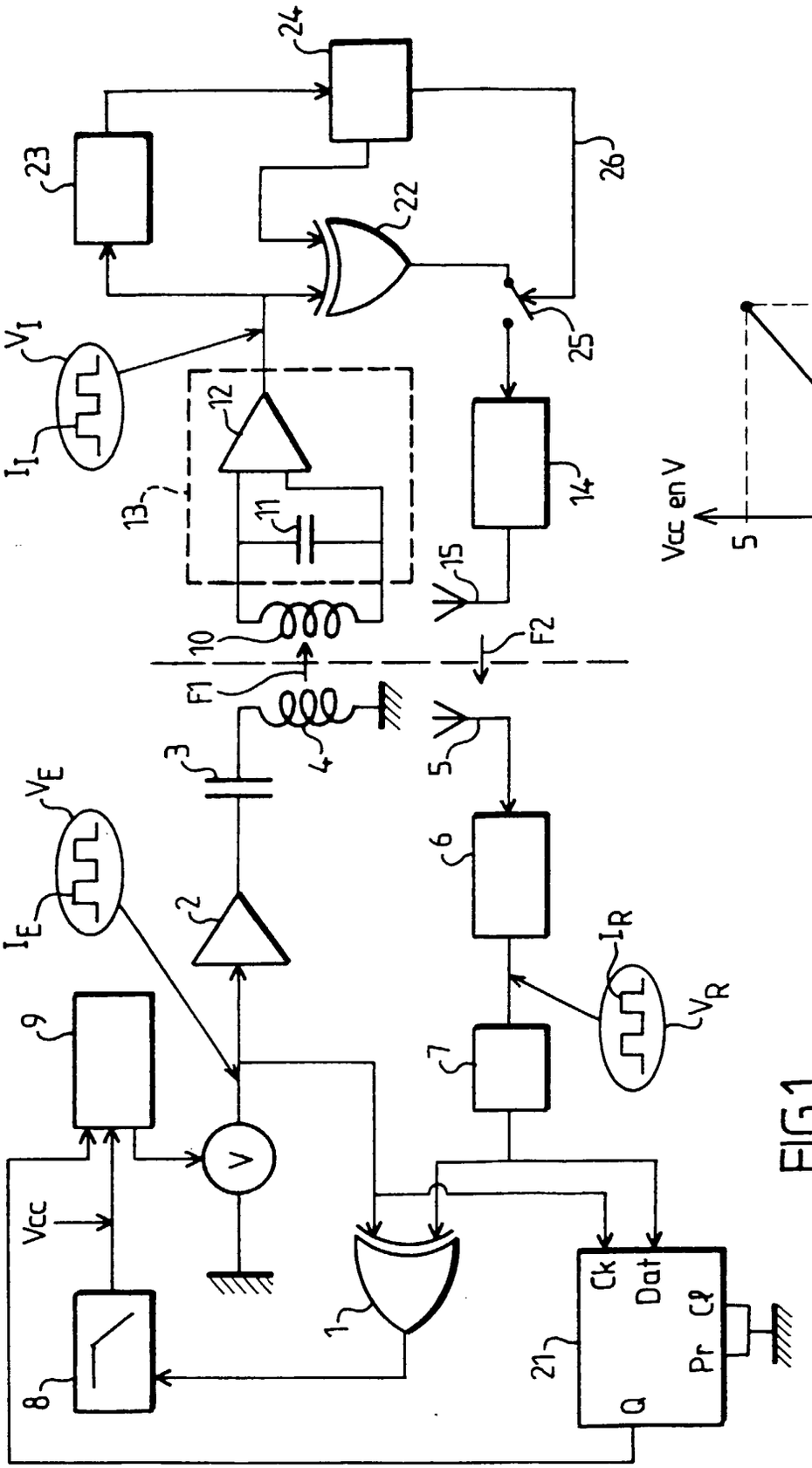
24
23
22
26
25
V_I
I_I
12
13
11
14
15
10
F1
F2
3
4
5
V_E
I_E
2
6
I_R
V_R
9
7
V
Vcc
8
1
21
Ck
Dat
Cl
Pr
Q

FIG.1

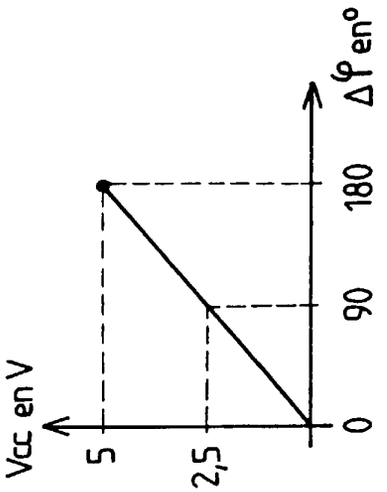
Vcc en V
5
2,5
0
90
180
Δφ en°

FIG.2

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 00 40 1666

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (Int.Cl.7)
A	FR 2 621 134 A (MATSUSHITA ELECTRIC WORKS LTD) 31 mars 1989 (1989-03-31) * abrégé * * page 3, ligne 10 - page 4, ligne 3 * * revendications; figures *	1-3,5,9	E05B49/00 G07C9/00
A	EP 0 694 887 A (SUISSE ELECTRONIQUE MICROTECH) 31 janvier 1996 (1996-01-31) * abrégé * * colonne 1, ligne 56 - colonne 2, ligne 48 * * revendications; figures *	1-3	
A	US 4 804 961 A (HANE BENGT) 14 février 1989 (1989-02-14) * abrégé * * colonne 2, ligne 44 - colonne 3, ligne 48 * * figures 1,2 *	1	
A	US 5 616 966 A (FISCHER ARMIN ET AL) 1 avril 1997 (1997-04-01)		DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7) E05B G07C B60R

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
LA HAYE	27 septembre 2000	Miltgen, E

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 00 40 1666

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

27-09-2000

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2621134 A	31-03-1989	JP 1182778 A	20-07-1989
		JP 2655660 B	24-09-1997
		JP 1182779 A	20-07-1989
		JP 2603672 B	23-04-1997
		JP 1272328 A	31-10-1989
		JP 1084175 A	29-03-1989
		JP 1084174 A	29-03-1989
		DE 3832409 A	06-04-1989
		GB 2210538 A,B	07-06-1989
		KR 9204754 B	15-06-1992
		US 4899158 A	06-02-1990
EP 0694887 A	31-01-1996	FR 2723238 A	02-02-1996
		DE 69512719 D	18-11-1999
		DE 69512719 T	18-05-2000
US 4804961 A	14-02-1989	SE 456118 B	05-09-1988
		AT 67864 T	15-10-1991
		DE 3681734 A	31-10-1991
		DE 3681734 D	31-10-1991
		EP 0249638 A	23-12-1987
		JP 63501981 T	04-08-1988
		NO 873301 A	06-08-1987
		SE 8505888 A	13-06-1987
		WO 8703698 A	18-06-1987
US 5616966 A	01-04-1997	EP 0710756 A	08-05-1996

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82