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

(11) EP 1 688 888 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
09.08.2006 Bulletin 2006/32

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

(21) Numéro de dépôt: **05100803.5**

(22) Date de dépôt: **04.02.2005**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU MC NL PL PT RO SE SI SK TR
Etats d'extension désignés:
AL BA HR LV MK YU

(71) Demandeur: **Sokymat Automotive GmbH**
51580 Reichshof-Wehnrath (DE)

(72) Inventeurs:
- **URBAN, Volker**
  51709, Marienheide (DE)
- **GYGER, Thomas**
  2316, Les Ponts-de-Martel (CH)

(74) Mandataire: **Vigand, Philippe et al**
ICB,
Ingénieurs Conseils en Brevets SA,
Rue des Sors 7
2074 Marin (CH)

(54) Procédé de communication et de contrôle de données d'authentification entre un dispositif portable à transpondeur et une unité de lecture d'un véhicule

(57) Le procédé permet de communiquer et de contrôler des données d'authentification entre un dispositif à transpondeur (1) et une unité de lecture (2) d'un véhicule pour autoriser l'accès au véhicule. Le dispositif comprend un circuit logique (11), une mémoire non-volatile (13), un circuit de cryptage et/ou de décryptage (12) et un module d'émission et de réception (14, 16) de signaux de données (S_D). L'unité de lecture comprend une unité à microprocesseur (21), une mémoire (22), un générateur de nombres aléatoires (24) et un second module d'émission et de réception (23, 25) de signaux de données (S_D). Un nombre aléatoire (RN1) généré dans l'unité de lecture est transmis avec une première fonction cryptée à l'aide du premier nombre aléatoire et une clé secrète. Le dispositif à transpondeur reçoit le nombre aléatoire et la première fonction cryptée. Une nouvelle première fonction cryptée est calculée à l'aide d'une clé secrète identique à la clé secrète de l'unité de lecture dans le dispositif à transpondeur. Cette nouvelle première fonction est comparée à la première fonction cryptée reçue. Une seconde fonction cryptée est également calculée dans le dispositif à transpondeur afin d'être transmise à l'unité de lecture uniquement si la nouvelle première fonction cryptée est égale à la première fonction cryptée reçue. La validité de la seconde fonction cryptée est contrôlée dans l'unité de lecture afin d'autoriser l'accès au véhicule. Le nombre de bits du nombre aléatoire, des première et seconde fonctions cryptées peut être configuré dans le dispositif à transpondeur et/ou dans l'unité de lecture à une longueur désirée.

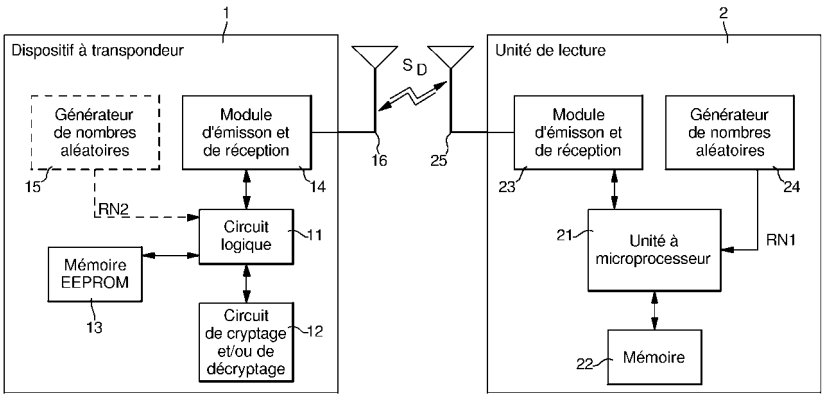

Fig. 1

EP 1 688 888 A1

Description

[0001] L'invention concerne un procédé de communication et de contrôle sans fil de données d'authentification entre un dispositif à transpondeur et une unité de lecture de préférence disposée dans un véhicule. Le dispositif à transpondeur comprend notamment un circuit logique, une mémoire, un module d'émission et de réception de signaux de données et un circuit de cryptage et/ou de décryptage, alors que l'unité de lecture comprend une unité à microprocesseur, une mémoire, un générateur de nombres aléatoires ainsi qu'un module d'émission et de réception de signaux de données. De cette manière, un échange de données d'authentification peut être effectué entre le dispositif à transpondeur personnalisé et l'unité de lecture correspondante de manière à autoriser l'accès au véhicule.

[0002] Après avoir passé par toutes les opérations nécessaires d'authentification ou d'identification, le dispositif à transpondeur est en mesure de commander certaines fonctions du véhicule. Ces fonctions peuvent être par exemple la commande de verrouillage ou déverrouillage de portes et/ou vitres du véhicule, la commande de démarrage du véhicule, une fonction d'immobilisation dudit véhicule, ou d'autres commandes.

[0003] La transmission ou communication sans fil de données à l'aide de signaux électromagnétiques entre un dispositif à transpondeur et une unité de lecture placée dans un véhicule est bien connue. Il peut s'agir de signaux à basse fréquence ou radiofréquences.

[0004] Habituellement dans un mode simple d'authentification entre un transpondeur et lecteur, il est transmis tout d'abord du lecteur au transpondeur une fois que ce dernier a été activé, un signal d'interrogation qui peut comprendre des données relatives à un nombre aléatoire à m bits, par exemple à 56 bits, suivi de données cryptées à n bits, par exemple à 28 bits. Le transpondeur reçoit et démodule le signal de données. Le transpondeur peut décrypter les données cryptées à contrôler et effectuer une opération de cryptage en continu pour obtenir d'autres données cryptées sur la base d'une clé secrète et du nombre aléatoire reçu. Après vérification des données cryptées reçues, le transpondeur transmet au lecteur les autres données cryptées afin qu'elles puissent être contrôlées dans le lecteur. Une fois que toutes les vérifications ont été effectuées avec succès, le transpondeur est susceptible de commander diverses fonctions du véhicule.

[0005] Le nombre de bits du nombre aléatoire transmis et le nombre de bits des données cryptées sont généralement fixés pour la communication et le contrôle des données d'authentification. Un laps de temps est plus ou moins déterminé pour cette procédure d'authentification, qui peut être fonction également de la distance séparant les deux unités.

[0006] Normalement le dispositif à transpondeur ne doit pas être trop éloigné du véhicule pour pouvoir échanger des données d'authentification avec l'unité de lecture du véhicule. Principalement, la fréquence porteuse des signaux échangés est une basse fréquence par exemple voisine de 125 kHz. De ce fait, il est nécessaire que le dispositif à transpondeur ne soit pas éloigné de plus de 2 à 3 m du véhicule pour opérer une ou plusieurs commandes après authentification.

[0007] Plusieurs algorithmes de cryptage utilisés habituellement possèdent l'inconvénient d'être relativement compliqués à mettre en oeuvre dans l'unité de lecture et principalement dans le dispositif à transpondeur, qui est en général de type passif. Un temps de contrôle du procédé d'authentification est de ce fait relativement long.

[0008] L'invention a pour but principal de fournir un procédé de communication et de contrôle sans fil de données d'authentification entre un dispositif à transpondeur et une unité de lecture en utilisant une méthode de cryptage et/ou décryptage et de transmission simplifiée et facilement configurable.

[0009] A cet effet, l'invention concerne un procédé de communication et de contrôle sans fil de données d'authentification selon les caractéristiques des revendications indépendantes 1 et 8.

[0010] Des formes avantageuses de l'invention sont définies dans les revendications dépendantes 2 à 7.

[0011] Un avantage du procédé de communication et de contrôle de données d'authentification réside dans le fait que le dispositif à transpondeur, ainsi que l'unité de lecture peuvent être configurés de telle manière à adapter la longueur des données d'authentification à transmettre. La longueur des données est définie par un nombre déterminé de bits. Il peut être défini un nombre de bits déterminé pour la transmission d'un ou plusieurs nombres aléatoires, et un nombre de bits équivalent ou différent pour la transmission de fonctions de cryptage basées sur le ou les nombres aléatoires générés.

[0012] Les buts, avantages et caractéristiques du procédé de communication et de contrôle de données d'authentification entre un dispositif à transpondeur et une unité de lecture d'un véhicule apparaîtront mieux dans la description suivante d'au moins une forme d'exécution illustrée par les dessins sur lesquels :

la figure 1 représente de manière simplifiée des composants électroniques d'un dispositif portable à transpondeur et d'une unité de lecture pour des opérations d'authentification pour la mise en oeuvre du procédé selon l'invention,

la figure 2 représente de manière simplifiée des données échangées entre le dispositif à transpondeur et l'unité de lecture dans un mode de simple authentification du procédé selon l'invention,

la figure 3 représente de manière simplifiée des étapes d'authentification dans le transpondeur selon un mode de simple authentification du procédé selon l'invention,

la figure 4 représente de manière simplifiée une partie d'un circuit logique et d'un circuit de cryptage du

transpondeur dans un mode de simple authentification pour la mise en oeuvre du procédé selon l'invention,

la figure 5 représente de manière simplifiée des données échangées entre le dispositif à transpondeur et l'unité de lecture dans un mode d'authentification mutuelle du procédé selon l'invention,

la figure 6 représente de manière simplifiée des étapes d'authentification dans le transpondeur selon un mode d'authentification mutuelle du procédé selon l'invention, et

la figure 7 représente de manière simplifiée une partie d'un circuit logique et d'un circuit de cryptage du transpondeur dans un mode d'authentification mutuelle pour la mise en oeuvre du procédé selon l'invention.

[0013] La description suivante est relative à un procédé de communication et de contrôle sans fil de données d'authentification entre un dispositif à transpondeur et une unité de lecture disposée dans un véhicule pour autoriser l'accès au véhicule après contrôle. Il est à noter que tous les composants électroniques du dispositif portable à transpondeur et de l'unité de lecture pour la mise en oeuvre du procédé, qui sont bien connus d'un homme du métier dans ce domaine technique, ne seront pas expliqués en détail.

[0014] L'autorisation d'accès concerne aussi bien la commande de verrouillage ou déverrouillage des portes et fenêtres du véhicule, la commande des phares, la commande de démarrage du véhicule, la commande d'une alarme ou d'une immobilisation du véhicule, la commande du klaxon, la lecture de différents paramètres du véhicule ou d'autres commandes ou fonctions. Les signaux sont de préférence des signaux basse fréquence (125 kHz) pour une communication à courte distance, par exemple dans une zone séparant le dispositif à transpondeur de l'unité de lecture de l'ordre de 2 à 3 m. Dans ce cas, le transpondeur peut être du type passif, c'est-à-dire qu'il est électriquement alimenté grâce aux signaux transmis par l'unité de lecture.

[0015] Bien entendu, il pourrait aussi être imaginé d'employer des signaux radiofréquences à courte distance (434 MHz) pour établir une telle communication. Cependant avec de tels signaux, il est constaté une plus forte consommation électrique, ce qui nécessiterait plutôt l'emploi d'un transpondeur du type actif.

[0016] La figure 1 représente de manière simplifiée un dispositif à transpondeur 1 susceptible d'établir une communication avec une unité de lecture 2 pour la mise en oeuvre du procédé selon l'invention lorsque le dispositif se trouve dans une zone déterminée autour de l'unité de lecture. Pour ce faire, le dispositif portable à transpondeur 1 peut prendre la forme d'un badge, d'une bague, d'une montre-bracelet, d'une ceinture, d'un téléphone portable ou de tout autre objet de petite dimension facilement transportable.

[0017] Le dispositif portable à transpondeur 1 comprend essentiellement un circuit logique 11, qui définit une machine d'état ou logique câblée, pour la gestion des diverses opérations effectuées dans le transpondeur. Le dispositif à transpondeur 1 comprend encore reliés au circuit logique 11, un circuit de cryptage et/ou de décryptage 12, une mémoire non-volatile 13 par exemple du type EEPROM, un module d'émission et de réception 14 de signaux de données S_D qui sont transmis et reçus par une antenne 16 reliée au module 14, ainsi qu'un générateur 15 de nombres aléatoires RN2. Les signaux de données peuvent comprendre des données codées et des données publiques. Dans un mode de simple authentification du dispositif et de l'unité de lecture pour le procédé selon l'invention, le générateur de nombres aléatoires 15 du dispositif à transpondeur 1 peut être omis comme montré en traits interrompus sur la figure 1.

[0018] Le circuit de cryptage et/ou de décryptage 12, qui sera expliqué de manière plus détaillée notamment en référence aux figures 4 et 7, est de préférence configuré en circuit de cryptage par le circuit logique 11 et des paramètres mémorisés dans la mémoire EEPROM 13. Ce circuit de cryptage configuré permet d'effectuer un codage par blocs d'un nombre aléatoire à l'aide d'une clé secrète de cryptage mémorisée dans la mémoire 13 afin d'obtenir une fonction cryptée sur la base du nombre aléatoire. Chaque bloc à crypter dans le circuit de cryptage 12 représente un nombre déterminé de bits du nombre aléatoire. L'algorithme de cryptage peut par exemple être du type DES qui est bien connu dans ce domaine technique.

[0019] L'unité de lecture 2 comprend principalement une unité à microprocesseur 21 pour le traitement par logiciel de toutes les opérations effectuées dans l'unité de lecture. L'unité de lecture 2 comprend encore reliés à l'unité à microprocesseur 21, une mémoire 22 de données et/ou paramètres, un générateur 24 de nombres aléatoires RN1, ainsi qu'un module 23 d'émission et de réception de signaux de données S_D qui sont transmis et reçus par une antenne 25 reliée au module 23. Les signaux de données S_D, qui comprennent des données modulées sur une fréquence porteuse, sont démodulés dans le module 23 afin que l'unité à microprocesseur 21 puisse traiter de manière connue les données démodulées.

[0020] La mémoire EEPROM 13 du dispositif à transpondeur 1 permet d'enregistrer dans certaines positions de la mémoire notamment un ou plusieurs nombres aléatoires par exemple de 128 bits chacun, une ou plusieurs clés secrètes de cryptage, différents paramètres de configuration, et d'autres données. Ces paramètres de configuration, qui peuvent être introduits soit en fin des étapes de production du dispositif à transpondeur, soit en cours d'utilisation du dispositif à transpondeur, concernent par exemple la configuration du circuit logique 11 de manière à déterminer la longueur des données d'authentification à échanger avec l'unité de lecture.

[0021] Cette longueur de données est définie comme

un nombre déterminé de bits à transmettre, que ce soit la transmission d'un nombre aléatoire généré ou une fonction calculée relative au nombre aléatoire généré. Ce nombre de bits est de préférence un multiple de 8. De cette manière, le dispositif à transpondeur 1 peut être configuré à choix pour transmettre une longueur de données correspondant à 32 bits, 64 bits, 96 bits ou 128 bits, ce qui constitue une caractéristique principale du procédé selon l'invention, comme expliqué dans la suite de la description.

[0022] Bien entendu, une longueur de chaque paquet de données à échanger peut être choisie plus grande que 128 bits dans le cas où le transpondeur est susceptible de traiter des mots binaires plus grands que 128 bits, par exemple de 196 ou 256 bits.

[0023] Lorsque le dispositif à transpondeur personnalisé 1, ainsi que l'unité de lecture 2 correspondante sont configurés pour un échange de paquets de données de longueur égale à 32 bits, il est possible d'accélérer la procédure d'authentification pour autoriser plus rapidement après contrôle l'accès au véhicule. Cependant, avec une telle longueur du paquet de données, la sécurité est moins grande qu'avec un nombre de bits plus important, mais peut être jugée néanmoins suffisante.

[0024] Les signaux de données d'authentification, qui sont échangés entre le dispositif à transpondeur personnalisé et l'unité de lecture correspondante sont expliqués ci-dessous en référence à la figure 2. Le contrôle d'autorisation d'accès au véhicule du dispositif à transpondeur peut être effectué par un procédé à simple authentification.

[0025] Une fois que le dispositif à transpondeur 1 a été activé, c'est-à-dire mis en fonction sur la base de précédents signaux d'interrogation reçus de l'unité de lecture 2, l'unité de lecture génère un nombre aléatoire RN1 et calcule une première fonction cryptée F(RN1) à l'aide d'une clé secrète et du nombre aléatoire RN1 généré. L'unité de lecture 2 transmet le nombre aléatoire RN1 suivi de la première fonction cryptée F(RN1) à destination du dispositif à transpondeur 1.

[0026] Le dispositif à transpondeur 1 démodule le signal reçu de l'unité de lecture dans son module de réception et d'émission pour prélever le nombre aléatoire reçu, ainsi que la première fonction cryptée reçue. Dès la réception du nombre aléatoire et de la première fonction cryptée, ou après avoir validé la première fonction, le dispositif à transpondeur peut transmettre à l'unité de lecture un signal ACK validant la réception des données. Toutefois, cette étape n'est pas toujours nécessaire, c'est pourquoi elle est représentée sur la figure 2 en traits interrompus.

[0027] Après avoir contrôlé la validité de la fonction cryptée F(RN1) reçue à l'aide du nombre aléatoire RN1, le dispositif à transpondeur calcule une seconde fonction de cryptage G(RN1) à l'aide d'une clé secrète équivalente à l'unité de lecture et du nombre aléatoire reçu. L'unité de lecture reçoit et démodule le signal codé reçu du dispositif à transpondeur afin de contrôler la validité de la seconde fonction de cryptage G(RN1) à l'aide de ladite clé secrète et du nombre aléatoire généré RN1.

[0028] Pour mieux comprendre les diverses opérations effectuées dans le dispositif à transpondeur 1 du procédé d'authentification, on se réfèrera ci-après à la figure 3.

[0029] Comme expliqué ci-dessus, le dispositif à transpondeur est premièrement activé à l'étape 30 avant de recevoir tout d'abord le nombre aléatoire RN 1 fourni par l'unité de lecture à l'étape 31. Ce nombre aléatoire est placé dans un registre d'entrée du dispositif à transpondeur. A l'étape 32, le dispositif à transpondeur reçoit la première fonction cryptée F(RN1) qu'il place dans un autre registre.

[0030] Le dispositif à transpondeur doit être en mesure de recalculer la première fonction de cryptage à l'aide d'une clé secrète équivalente à la clé secrète de l'unité de lecture et du nombre aléatoire reçu. Pour ce faire à l'étape 33, le nombre aléatoire RN1 du registre d'entrée est fourni à une unité de cryptage du circuit de cryptage. Cette unité de cryptage reçoit également la clé secrète afin de crypter par bloc de bits le mot binaire du registre, qui est composé du nombre aléatoire de dimension configurée et de bits de remplissage provenant de la mémoire EEPROM pour remplir complètement le registre d'entrée de dimension définie.

[0031] La première fonction F'(RN1) recalculée par l'unité de cryptage est comparée à l'étape 34 à la première fonction cryptée F(RN1) reçue. Si les deux premières fonctions sont égales, alors le dispositif peut transmettre à l'unité de lecture une confirmation de réception correcte ACK à l'étape 35. Par contre, si les deux premières fonctions ne correspondent pas, alors le dispositif peut transmettre une annonce de réception incorrecte NACK à l'unité de lecture à l'étape 37. Toutefois, les étapes 35 et 37 ne sont pas forcément nécessaires, c'est pourquoi elles sont représentées chacune dans un cadre en traits interrompus.

[0032] En plus de la première fonction recalculée F' (RN1) à l'étape 33, une seconde fonction de cryptage peut être également calculée dans l'unité de cryptage du dispositif à transpondeur. Cette seconde fonction de cryptage est placée momentanément dans un registre avant d'être transmise à l'unité de lecture à l'étape 36 uniquement si les premières fonctions cryptées sont égales. A la suite de l'envoi de la seconde fonction cryptée G(RN1) de l'étape 36, le procédé d'authentification au niveau du dispositif à transpondeur se termine à l'étape 38.

[0033] En référence à la figure 4, il est expliqué les éléments du circuit logique et du circuit de cryptage nécessaires au calcul des fonctions de cryptage dans le dispositif à transpondeur. Sur cette figure 4, le circuit de cryptage est composé essentiellement d'une unité de cryptage 41, d'un registre d'entrée 40 et d'un registre de sortie 42.

[0034] Dès la réception du nombre aléatoire RN1 provenant de l'unité de lecture, ce nombre aléatoire est placé

dans un registre d'entrée 40 du circuit de cryptage. Le registre d'entrée est de dimension déterminée pour pouvoir recevoir un mot binaire de 128 bits par exemple. Si le nombre aléatoire RN1 est composé d'un nombre configuré de bits inférieur par exemple 32 bits ou 64 bits ou 96 bits, le registre d'entrée devra être complété par des bits de remplissage BR provenant de la mémoire EEPROM sous la commande du circuit logique. Le nombre aléatoire occupera une portion 40b du registre d'entrée alors que les bits de remplissage BR occuperont une portion 40a du registre d'entée 40.

[0035] A l'aide d'un algorithme de cryptage, qui peut être du type DES, une opération de cryptage par blocs à l'aide d'une clé secrète Key tirée de la mémoire est effectuée dans l'unité de cryptage 41. Le résultat de l'opération de cryptage est placé dans un registre de sortie 42 de dimension équivalente à la dimension du registre d'entrée. Le nombre de bits contenu dans le registre de sortie 42 est un multiple de 8, par exemple 128 bits. Le nombre de bits du registre de sortie 42 sont répartis en quatre groupes de bits A, B, C, D, placés dans quatre portions successives 42a, 42b, 42c, 42d du registre de sortie 42. Chaque groupe de bits est composé de 32 bits si le registre de sortie peut comprendre 128 bits.

[0036] La première fonction de cryptage recalculée F' (RN1) placée dans un registre 46 est obtenue par combinaison des premier et troisième groupes de bits A et C du registre de sortie 42 à travers un opérateur de réduction 44 du circuit logique. La seconde fonction cryptée G (RN1) placée dans un registre 47 est obtenue par combinaison des second et quatrième groupes de bits B et D du registre de sortie 42 à travers un opérateur de réduction 45. Dans ce cas, les première et seconde fonctions cryptées F'(RN1) et G(RN1) comprennent 32 bits.

[0037] A l'aide de différents opérateurs ou d'un nombre de groupes de bits différent du registre de sortie 42, il est possible de configurer la dimension ou longueur voulue de chaque fonction cryptée. Par exemple pour obtenir une dimension de 64 bits pour chaque fonction, il est possible de combiner à l'aide d'opérateurs de réduction deux paires de groupes de bits du registre de sortie.

[0038] Finalement dans une configuration où le nombre aléatoire RN1 est composé de 128 bits, et que les fonctions cryptées sont également composées de 128 bits, le premier résultat de l'opération de cryptage placé dans le registre de sortie 42 donne la première fonction de cryptage F'(RN1). Cette première fonction cryptée est placée par le chemin b montré en traits interrompus dans le registre 46. Pour le calcul de la seconde fonction de cryptage G(RN1), la première fonction recalculée F' (RN1) remplace le nombre aléatoire dans le registre d'entrée 40 montré par le chemin a en traits interrompus. Le second résultat de l'opération de cryptage placée dans le registre de sortie 42 donne la seconde fonction de cryptage G(RN1), qui est placée dans le registre 47 montré par le chemin c en traits interrompus.

[0039] On comprend qu'il est facile de configurer le nombre de bits du nombre aléatoire ou de chaque fonction de cryptage pour le procédé d'authentification selon l'invention.

[0040] Aux figures 5 à 7, il est décrit les différentes étapes du procédé de communication et de contrôle de données d'authentification entre un dispositif à transpondeur 1 personnalisé et une unité de lecture 2 d'un véhicule. Toutefois à la différence du procédé décrit ci-devant, il est réalisé une procédure d'authentification mutuelle avant d'autoriser l'accès au véhicule si le dispositif personnalisé est reconnu. Cette authentification mutuelle est réalisée sur la base d'un premier nombre aléatoire généré dans l'unité de lecture et d'un second nombre aléatoire généré dans le dispositif à transpondeur.

[0041] Comme on peut le voir à la figure 5, une fois que le dispositif à transpondeur est activé, il peut premièrement transmettre un signal ACK pour annoncer à l'unité de lecture sa mise en fonction. Cependant cette étape comme précédemment montrée en traits interrompus n'est pas indispensable. Le dispositif à transpondeur génère un second nombre aléatoire RN2, qu'il transmet à l'unité de lecture. Dès réception du second nombre aléatoire RN2, l'unité de lecture 2 transmet au dispositif à transpondeur 1 un premier nombre aléatoire généré dans l'unité de lecture, ainsi qu'une première fonction cryptée F(RN1,RN2) obtenue à l'aide d'une clé secrète et des deux nombres aléatoires RN1 et RN2.

[0042] A la réception du première nombre aléatoire RN1 et de la première fonction cryptée F(RN1,RN2), le dispositif doit calculer une même première fonction de cryptage. Si les deux premières fonctions de cryptage sont équivalentes, une seconde fonction de cryptage G (RN1,RN2) est calculée à l'aide de la même clé secrète et des deux nombres aléatoires RN1 et RN2. Cette seconde fonction cryptée est transmise à l'unité de lecture de manière à lui permettre de retrouver cette seconde fonction afin de terminer le procédé d'authentification et autoriser l'accès au véhicule.

[0043] La figure 6 montre les différentes étapes du procédé d'authentification dans le dispositif à transpondeur.

[0044] Après avoir activé le dispositif à transpondeur à l'étape 60, un signal ACK pour annoncer à l'unité de lecture sa mise en fonction peut être transmis à l'étape 61, et un second nombre aléatoire généré dans le dispositif est transmis à l'étape 62 à l'unité de lecture. Toutefois, l'étape 61 n'est pas forcément nécessaire, c'est pourquoi elle est montrée dans un cadre en traits interrompus.

[0045] Le dispositif à transpondeur reçoit de l'unité de lecture le premier nombre aléatoire RN1 à l'étape 63, et la première fonction cryptée F(RN1,RN2) à l'étape 64. A l'étape 65, la première fonction de cryptage est recalculée à l'aide des deux nombres aléatoires pour donner une première fonction recalculée F'(RN1,RN2) à comparer à la première fonction cryptée F(RN1,RN2) reçue à l'étape 66. Si les deux premières fonctions de cryptage sont égales, il peut être transmis un signal ACK de confirmation de réception correcte à l'étape 67. Par contre si les deux premières fonctions sont différentes, il peut

être transmis un signal NACK relatif à une réception incorrecte à l'étape 69. Toutefois, les étapes 67 et 69 ne sont pas forcément nécessaires, c'est pourquoi elles sont représentées chacune dans un cadre en traits interrompus.

[0046] En plus de la première fonction recalculée F' (RN1,RN2) à l'étape 65, une seconde fonction de cryptage G(RN1,RN2) peut être également calculée dans l'unité de cryptage du dispositif à transpondeur. Cette seconde fonction de cryptage est placée momentanément dans un registre avant d'être transmise à l'unité de lecture à l'étape 68 uniquement si les premières fonctions cryptées sont égales. Après l'envoi de la seconde fonction cryptée G(RN1,RN2) à l'étape 68, le procédé d'authentification mutuelle au niveau du dispositif à transpondeur se termine à l'étape 70.

[0047] La figure 7 représente des éléments équivalents aux éléments du circuit logique et du circuit de cryptage décrits à la figure 4. De ce fait, uniquement les différences essentielles sont expliquées ci-après.

[0048] Comme, il est généré deux nombres aléatoires RN1 et RN2, ils sont placés dans un même registre d'entrée 71, qui comprend une portion 71a pour des bits de remplissage, une portion 71b pour le premier nombre aléatoire RN1 et une portion 71c pour le second nombre aléatoire RN2. De préférence, chaque nombre aléatoire est composé de 32 bits, alors que le registre d'entrée 71 peut comprendre 128 bits.

[0049] Une opération de cryptage par blocs est effectuée dans l'unité de cryptage 72 à l'aide de la clé secrète et des bits du registre d'entrée. Le résultat du cryptage est placé dans un registre de sortie 73 réparti en quatre groupes de bits A, B, C, D placés successivement dans des portions 73a, 73b, 73c, 73d de 32 bits chacun.

[0050] La première fonction recalculée F'(RN1,RN2) est obtenue par combinaison des groupes A et C par l'intermédiaire d'un opérateur de réduction 74 du circuit logique et placée dans le registre 76. La seconde fonction de cryptage G(RN1,RN2) est obtenue par combinaison des groupes B et D par l'intermédiaire d'un opérateur de réduction 75 du circuit logique et placée par une sortie séquentielle dans le registre 77. Dans ce cas, les fonctions de cryptage sont composées de 32 bits.

[0051] Bien entendu, comme expliqué en référence à la figure 4, une configuration différente peut être effectuée pour obtenir des fonctions de cryptage à 64 bits ou à 128 bits sans qu'il soit nécessaire d'expliquer à nouveau la manière de les obtenir.

[0052] Dans une variante de réalisation non illustrée, il peut être concevable de configurer par exemple le dispositif à transpondeur de manière que le circuit de cryptage et/ou de décryptage soit configuré également pour décrypter une fonction cryptée. Pour ce faire, l'unité de cryptage précédemment décrite doit être en mesure d'effectuer une opération inverse à savoir décrypter une fonction cryptée à l'aide de la clé secrète pour retrouver le nombre aléatoire ayant servi au calcul de cette fonction cryptée.

[0053] Avant de générer une seconde fonction cryptée dans le dispositif à transpondeur, il peut être effectué une comparaison entre le premier nombre aléatoire reçu de l'unité de lecture avec un premier nombre aléatoire recalculé dans le circuit de décryptage à partir de la première fonction cryptée. Si les deux premiers nombres aléatoires sont égaux, la seconde fonction cryptée peut être transmise à l'unité de lecture.

[0054] A partir de la description qui vient d'être faite de multiples variantes de réalisation du procédé de communication et de contrôle de données d'authentification peuvent être conçues par l'homme du métier sans sortir du cadre de l'invention définie par les revendications. Il peut être prévu d'opérer automatiquement une configuration du nombre de bits qui compose soit chaque nombre aléatoire ou chaque fonction de cryptage durant l'établissement de la communication entre le dispositif à transpondeur et l'unité de lecture. Il peut être effectué un contrôle aussi bien d'un nombre aléatoire reçu qu'une fonction cryptée reçue dans le dispositif et/ou dans l'unité de lecture.

Revendications

1. Procédé de communication et de contrôle sans fil de données d'authentification entre un dispositif à transpondeur (1) et une unité de lecture (2) disposée notamment dans un véhicule de manière à autoriser l'accès au véhicule, le dispositif à transpondeur comprenant un circuit logique (11), une mémoire non-volatile (13), un circuit de cryptage et/ou de décryptage (12) et un premier module d'émission et de réception (14, 16) de signaux de données (S_D), l'unité de lecture comprenant une unité à microprocesseur (21), une mémoire (22), un générateur de nombres aléatoires (24) susceptible de fournir un premier nombre aléatoire (RN1) à l'unité à microprocesseur, et un second module d'émission et de réception (23, 25) de signaux de données (S_D),
   le procédé comprenant des étapes consistant à :

   a) transmettre un signal de données comprenant un premier nombre aléatoire (RN1) généré dans l'unité de lecture, le nombre de bits du nombre aléatoire à transmettre étant configuré à une première longueur désirée pour la transmission, et une première fonction cryptée (F(RN1)) sur la base d'une clé secrète et du premier nombre aléatoire, le nombre de bits de la première fonction cryptée étant configuré à une seconde longueur désirée pour la transmission,
   b) recevoir et démoduler le signal de données transmis (31, 32) par l'unité de lecture dans le dispositif à transpondeur,
   c) calculer (33) une nouvelle première fonction cryptée (F'(RN1)) dans le dispositif à transpondeur à l'aide du premier nombre aléatoire reçu

(RN1) et d'une clé secrète mémorisée dans la mémoire non-volatile (13) correspondant à la clé secrète de l'unité de lecture, la nouvelle première fonction cryptée étant calculée dans le circuit de cryptage à l'aide d'un algorithme de cryptage par blocs de bits,
d) comparer (34) la nouvelle première fonction cryptée à la première fonction cryptée reçue,
e) transmettre à l'unité de lecture une seconde fonction cryptée (G(RN1)) obtenue sur la base du premier nombre aléatoire (RN1) et de la clé secrète dans le circuit de cryptage (12), uniquement si la nouvelle première fonction cryptée est égale à la première fonction cryptée reçue, le nombre de bits de la seconde fonction cryptée étant configuré par le circuit logique à une troisième longueur désirée pour la transmission, et
f) contrôler la validité de la seconde fonction cryptée reçue dans l'unité de lecture afin d'autoriser l'accès au véhicule.

2. Procédé selon la revendication 1, **caractérisé en ce que** la longueur de chaque paquet de données échangées entre le dispositif à transpondeur et l'unité de lecture est composée d'un nombre de bits, qui est un multiple de 8.

3. Procédé selon la revendication 2, **caractérisé en ce que** la longueur de chaque paquet de données à transmettre peut être configurée à choix à 32 bits, à 64 bits, à 96 bits ou à 128 bits de manière à accélérer l'échange des données d'authentification plus la longueur de chaque paquet de données est faible.

4. Procédé selon l'une des revendications précédentes, **caractérisé en ce qu'**un signal de confirmation (ACK) de réception de données est transmis du dispositif à transpondeur à l'unité de lecture dès la réception du signal de données (S_D) de l'unité de lecture, ou après la comparaison de la première fonction cryptée (F(RN1)) et de la nouvelle première fonction cryptée (F'(RN1)).

5. Procédé selon l'une des revendications précédentes, **caractérisé en ce que** le premier nombre aléatoire reçu (RN1) dans le dispositif à transpondeur (1) est placé dans un registre d'entrée (40, 71) du circuit de cryptage (12) de dimension définie, par exemple de 128 bits, plus grande ou égale à la longueur configurée du premier nombre aléatoire, un certain nombre de bits de remplissage (BR) provenant de la mémoire non-volatile (13) étant placé dans le registre d'entrée afin de le compléter pour permettre à une unité de cryptage (41, 72) de crypter par blocs le mot binaire du registre d'entrée.

6. Procédé selon la revendication 5, **caractérisé en ce que** l'unité de cryptage (41, 72) fournit un résultat de cryptage dans un registre de sortie (42, 73) de dimension définie, par exemple de 128 bits, ce registre de sortie étant partitionnés en quatre groupes de bits (A, B, C, D) successifs, et **en ce que** la nouvelle première fonction cryptée (F'(RN1)) et la seconde fonction cryptée (G(RN1)) sont obtenues par combinaison différente de groupes de bits du registre de sortie à travers un opérateur respectif (44, 45; 74, 75) du circuit logique, les longueurs configurées des première et seconde fonctions cryptées étant égales.

7. Procédé selon l'une des revendications précédentes, dans lequel le dispositif à transpondeur comprend un autre générateur de nombres aléatoires (15) susceptible de fournir un second nombre aléatoire (RN2), **caractérisé en ce qu'**avant l'étape a), le dispositif à transpondeur transmet le second nombre aléatoire (RN2) à l'unité de lecture, **en ce que** l'unité de lecture calcule et transmet une première fonction cryptée (F(RN1,RN2)) sur la base d'une clé secrète et des premier et second nombres aléatoires (RN1, RN2), **en ce qu'**à l'étape c), une nouvelle première fonction cryptée (F'(RN1 ,RN2)) est calculée dans le dispositif à transpondeur à l'aide des premier et second nombres aléatoires reçus (RN1) et d'une clé secrète correspondant à la clé secrète de l'unité de lecture, et **en ce qu'**à l'étape e), le dispositif à transpondeur transmet à l'unité de lecture une seconde fonction cryptée (G(RN1,RN2)) obtenue sur la base des premier et second nombres aléatoires (RN1) et de la clé secrète dans le circuit de cryptage (12), uniquement si la nouvelle première fonction cryptée est égale à la première fonction cryptée reçue.

8. Procédé de communication et de contrôle sans fil de données d'authentification entre un dispositif à transpondeur (1) et une unité de lecture (2) disposée notamment dans un véhicule de manière à autoriser l'accès au véhicule, le dispositif à transpondeur comprenant un circuit logique (11), une mémoire non-volatile (13), un circuit de cryptage et/ou de décryptage (12) et un premier module d'émission et de réception (14, 16) de signaux de données (S_D), l'unité de lecture comprenant une unité à microprocesseur (21), une mémoire (22), un générateur de nombres aléatoires (24) susceptible de fournir un premier nombre aléatoire (RN1) à l'unité à microprocesseur, et un second module d'émission et de réception (23, 25) de signaux de données (S_D), le procédé comprenant des étapes consistant à :

a) transmettre un signal de données comprenant un premier nombre aléatoire (RN1) généré dans l'unité de lecture, le nombre de bits du nombre aléatoire à transmettre étant configuré à une première longueur désirée, et une première

fonction cryptée (F(RN1)) sur la base d'une clé secrète et du premier nombre aléatoire, le nombre de bits de la première fonction cryptée étant configuré à une seconde longueur désirée,

b) recevoir et démoduler le signal de données transmis (31, 32) par l'unité de lecture dans le dispositif à transpondeur,

c) décrypter (33) la première fonction cryptée (F (RN1)) dans le circuit de décryptage configuré à l'aide d'une clé secrète mémorisée dans la mémoire non-volatile (13) correspondant à la clé secrète de l'unité de lecture pour obtenir un nouveau premier nombre aléatoire,

d) comparer (34) le nouveau premier nombre aléatoire décrypté avec le premier nombre aléatoire reçu,

e) transmettre à l'unité de lecture une seconde fonction cryptée (G(RN1)) obtenue sur la base du premier nombre aléatoire (RN1) et de la clé secrète, uniquement si le nouveau premier nombre aléatoire est égal au premier nombre aléatoire reçu, le nombre de bits de la seconde fonction étant configuré par le circuit logique à une troisième longueur désirée, et

f) contrôler la validité de la seconde fonction cryptée reçue dans l'unité de lecture afin d'autoriser l'accès au véhicule.

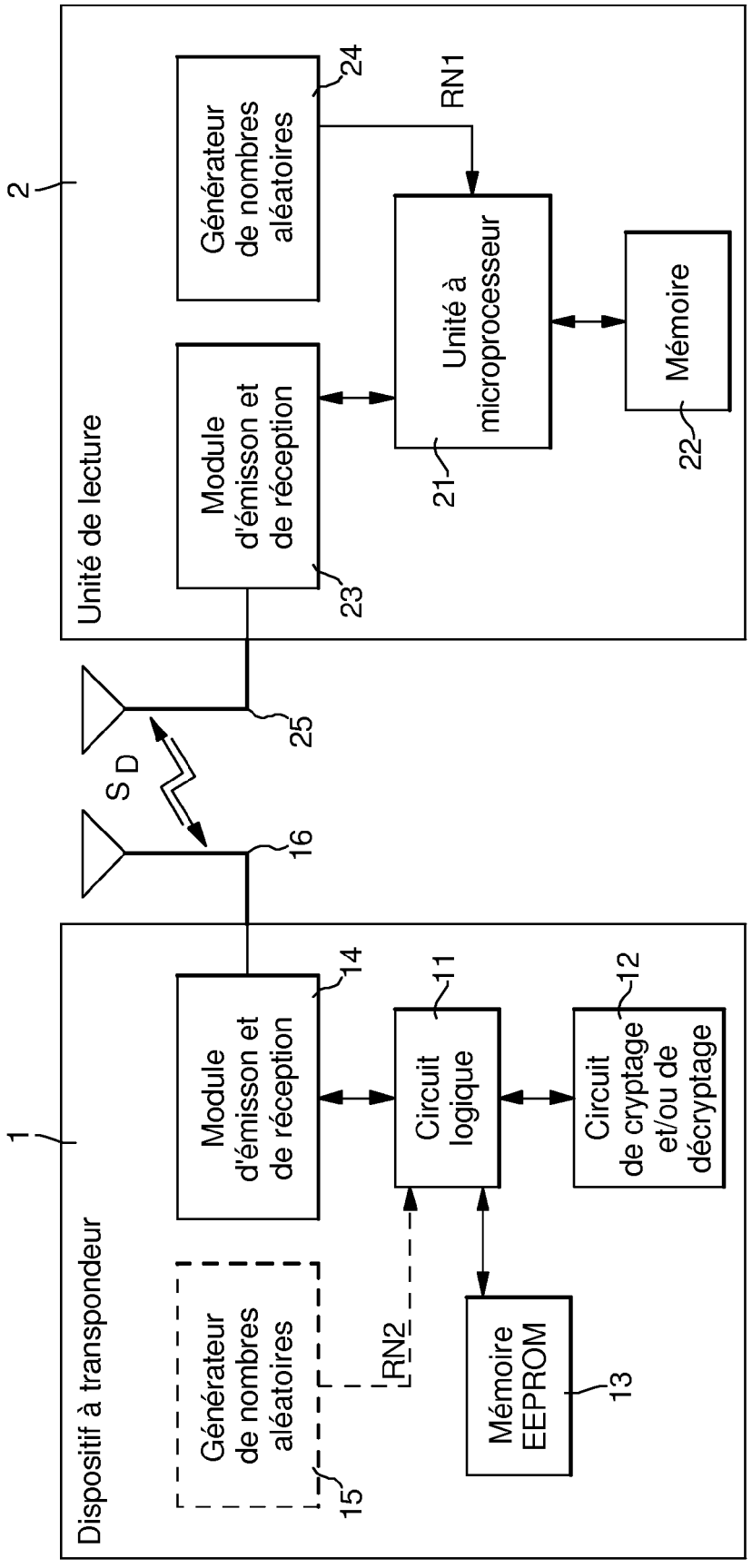
2
Unité de lecture
Générateur de nombres aléatoires
24
RN1
Module d'émisson et de réception
Unité à microprocesseur
Mémoire
23
21
22
25
S_D
16
1
Dispositif à transpondeur
Module d'émisson et de réception
14
Circuit logique
11
Circuit de cryptage et/ou de décryptage
12
Générateur de nombres aléatoires
15
RN2
Mémoire EEPROM
13

Fig. 1

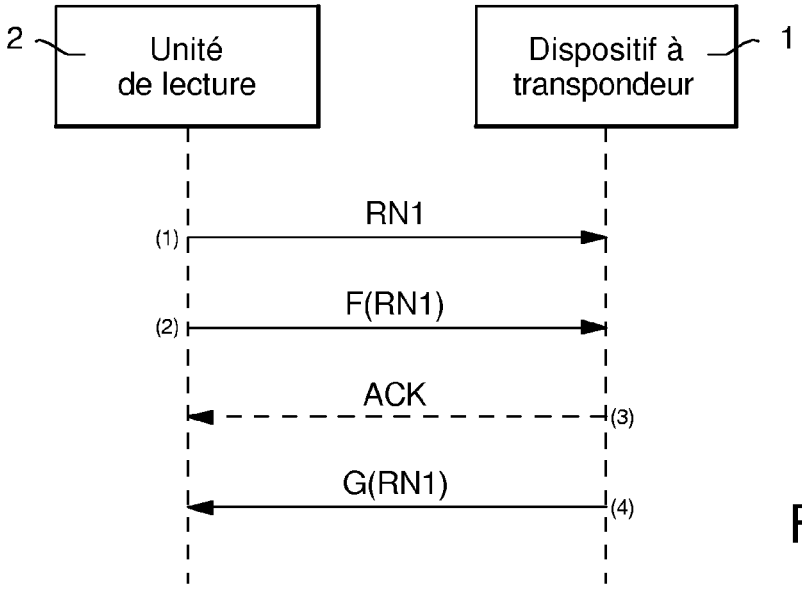
2
Unité de lecture
Dispositif à transpondeur
1
RN1
(1)
F(RN1)
(2)
ACK
(3)
G(RN1)
(4)

Fig. 2

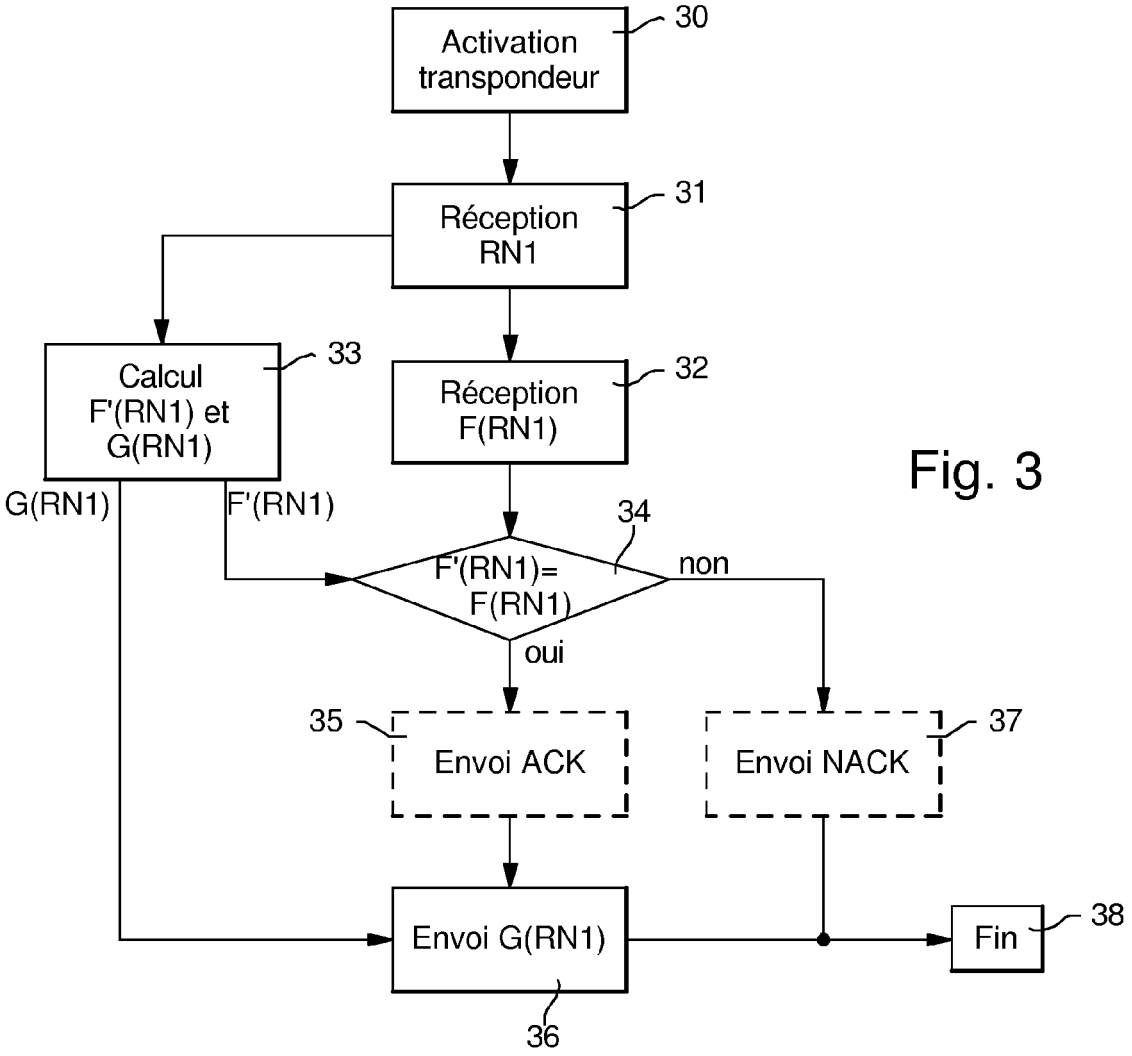
Activation transpondeur
30
Réception RN1
31
Calcul F'(RN1) et G(RN1)
33
Réception F(RN1)
32
G(RN1)
F'(RN1)
34
F'(RN1)= F(RN1)
non
oui
35
Envoi ACK
Envoi NACK
37
Envoi G(RN1)
36
Fin
38

Fig. 3

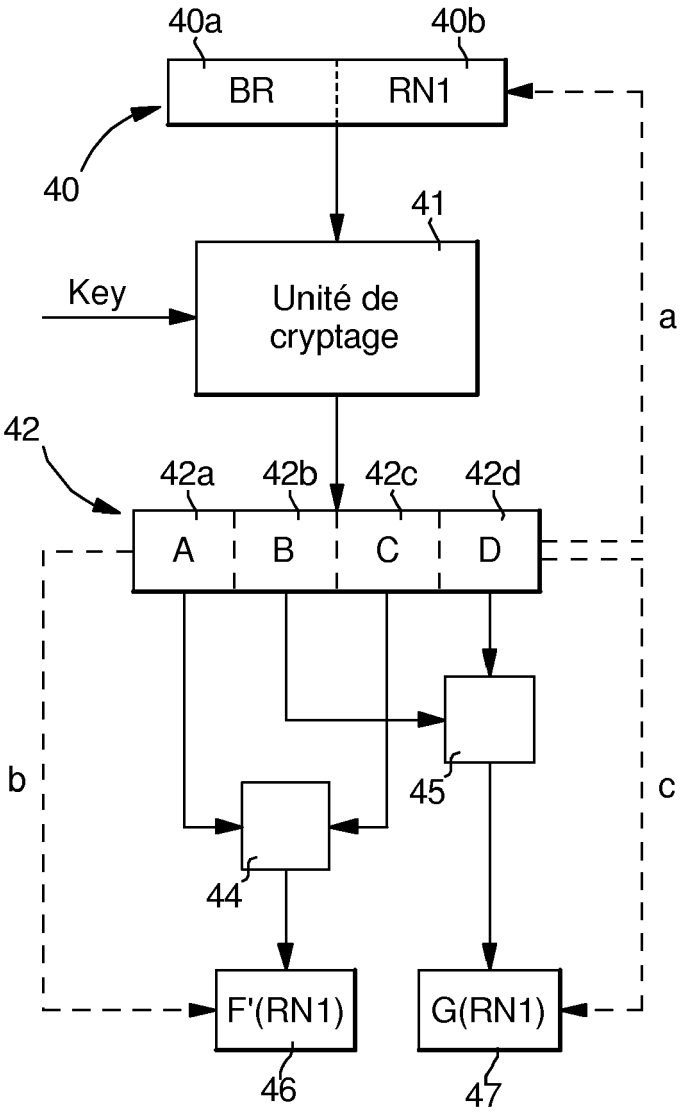
40a
40b
BR
RN1
40
41
Key
Unité de cryptage
a
42
42a
42b
42c
42d
A
B
C
D
b
c
45
44
F'(RN1)
G(RN1)
46
47

Fig. 4

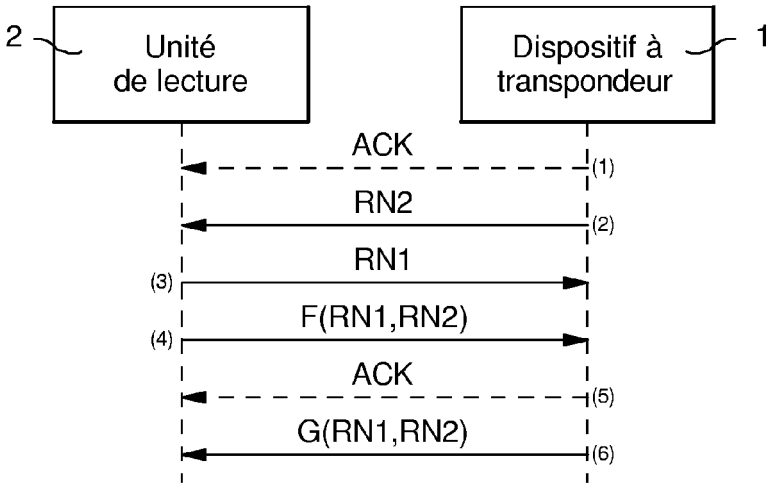
2
Unité de lecture
Dispositif à transpondeur
1
ACK
(1)
RN2
(2)
RN1
(3)
F(RN1,RN2)
(4)
ACK
(5)
G(RN1,RN2)
(6)

Fig. 5

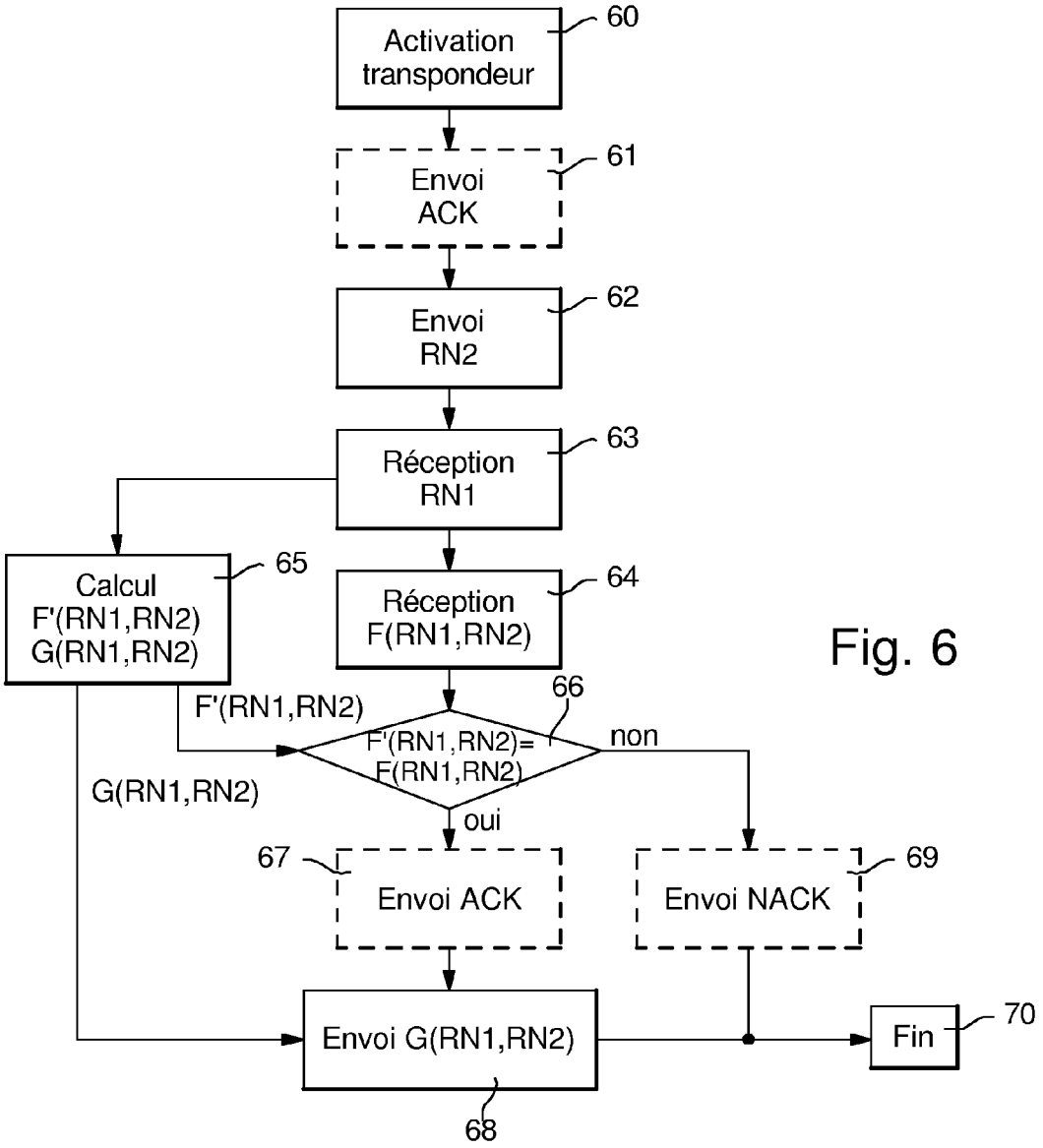
Activation transpondeur
60
Envoi ACK
61
Envoi RN2
62
Réception RN1
63
Calcul F'(RN1,RN2) G(RN1,RN2)
65
Réception F(RN1,RN2)
64
F'(RN1,RN2)
66
F'(RN1,RN2)= F(RN1,RN2)
non
G(RN1,RN2)
oui
67
Envoi ACK
Envoi NACK
69
Envoi G(RN1,RN2)
68
Fin
70

Fig. 6

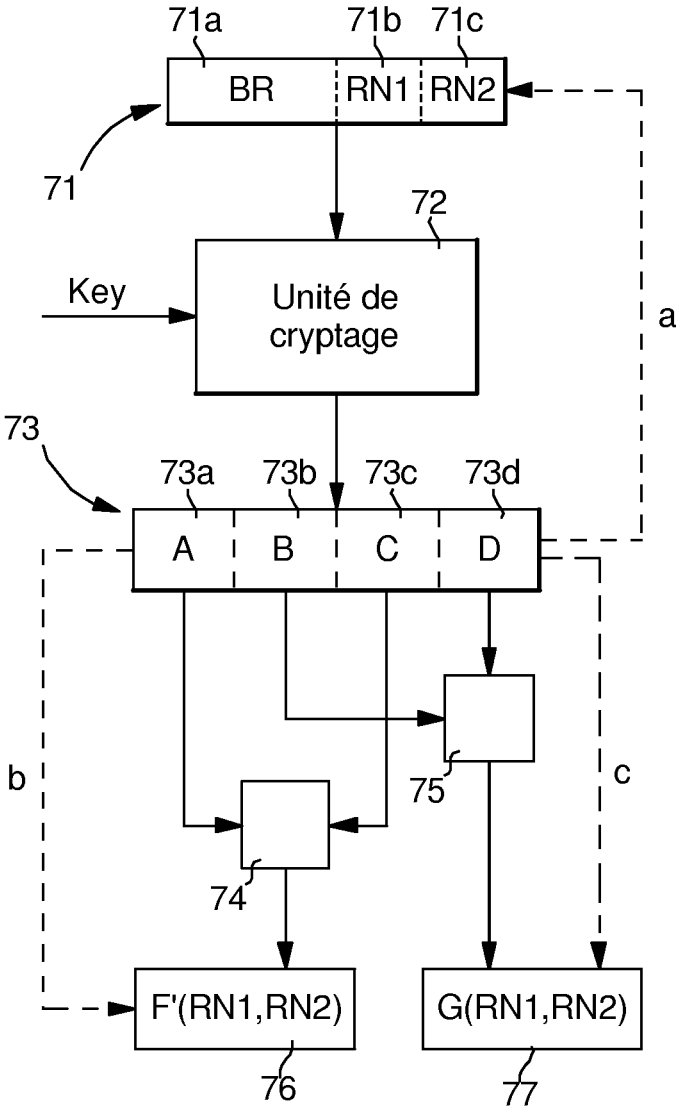
71a
71b
71c
BR
RN1
RN2
71
72
Key
Unité de cryptage
a
73
73a
73b
73c
73d
A
B
C
D
b
c
75
74
F'(RN1,RN2)
G(RN1,RN2)
76
77

Fig. 7

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 05 10 0803

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)
X Y	EP 0 923 054 A (DELPHI AUTOMOTIVE SYSTEMS DEUTSCHLAND GMBH; F + G MEGAMOS SICHERHEITSE) 16 juin 1999 (1999-06-16) * alinéa [0017] - alinéa [0018] * * figure 1 *	1,5,6,8 2-4,7	G07C9/00 B60R25/00
X	EP 1 443 469 A (DELPHI TECHNOLOGIES, INC) 4 août 2004 (2004-08-04) * alinéa [0029] - alinéa [0042] * * figure 1 *	1,5,6,8	
X	US 4 799 061 A (ABRAHAM ET AL) 17 janvier 1989 (1989-01-17) * colonne 3, ligne 4 - colonne 4, ligne 8 * * figure 2 *	1,8	
Y	EP 0 774 673 A (KABUSHIKI KAISHA TOKAI-RIKA-DENKI-SEISAKUSHO) 21 mai 1997 (1997-05-21) * colonne 2, ligne 30 - colonne 4, ligne 20 *	2,3	DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7) G07C
Y	US 6 075 454 A (YAMASAKI ET AL) 13 juin 2000 (2000-06-13) * colonne 2, ligne 33 - colonne 4, dernière ligne *	4	
Y	US 4 509 093 A (STELLBERGER ET AL) 2 avril 1985 (1985-04-02) * colonne 8, ligne 62 - colonne 11, ligne 9 * * figures 2,3 *	7	
A	US 2002/053027 A1 (KIM HEE-JUN) 2 mai 2002 (2002-05-02) * alinéa [0055] - alinéa [0062] * * figure 2 *	1-8	

-/--

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	7 juillet 2005	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)

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 05 10 0803

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	EP 1 387 323 A (OMEGA ELECTRONICS S.A) 4 février 2004 (2004-02-04) * alinéa [0031] - alinéa [0038] * * figure 2 *	1,8	
A	EP 0 492 692 A (DELCO ELECTRONICS CORPORATION) 1 juillet 1992 (1992-07-01)		

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.7)

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	7 juillet 2005	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

2

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 05 10 0803

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.

07-07-2005

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
EP 0923054	A	16-06-1999	DE	19815300 A1	17-06-1999
			DE	59808613 D1	10-07-2003
			EP	0923054 A2	16-06-1999
EP 1443469	A	04-08-2004	DE	10303960 A1	12-08-2004
			EP	1443469 A1	04-08-2004
US 4799061	A	17-01-1989	DE	3688316 D1	27-05-1993
			DE	3688316 T2	28-10-1993
			EP	0223122 A2	27-05-1987
			JP	1763604 C	28-05-1993
			JP	4051864 B	20-08-1992
			JP	62120564 A	01-06-1987
EP 0774673	A	21-05-1997	JP	9139985 A	27-05-1997
			JP	9149480 A	06-06-1997
			DE	69633165 D1	23-09-2004
			EP	0774673 A2	21-05-1997
			US	5844990 A	01-12-1998
US 6075454	A	13-06-2000	JP	11013320 A	19-01-1999
US 4509093	A	02-04-1985	DE	3225754 A1	12-01-1984
			DE	3372874 D1	10-09-1987
			EP	0098437 A2	18-01-1984
			ES	8605070 A1	01-08-1986
			JP	1689338 C	11-08-1992
			JP	3058031 B	04-09-1991
			JP	59048567 A	19-03-1984
US 2002053027	A1	02-05-2002	KR	2002024389 A	30-03-2002
			CN	1354110 A	19-06-2002
			DE	10147085 A1	18-07-2002
			JP	2002173002 A	18-06-2002
EP 1387323	A	04-02-2004	EP	1387323 A1	04-02-2004
EP 0492692	A	01-07-1992	US	5144667 A	01-09-1992
			AU	632721 B2	07-01-1993
			AU	8966491 A	25-06-1992
			DE	69112191 D1	21-09-1995
			DE	69112191 T2	04-01-1996
			EP	0492692 A2	01-07-1992
			JP	2095725 C	02-10-1996
			JP	4302682 A	26-10-1992
			JP	8006520 B	24-01-1996

EPO FORM P0460

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

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 05 10 0803

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.

07-07-2005

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0492692 A		KR 9501729 B1	28-02-1995

EPO FORM P0460

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