(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 743 386**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **97 00151**

(51) Int Cl[6] : E 05 B 49/00, B 60 R 25/04

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 09.01.97.

(30) **Priorité** : 09.01.96 DE 19600556.

(43) **Date de la mise à disposition du public de la demande :** 11.07.97 Bulletin 97/28.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SIEMENS AG* — DE.

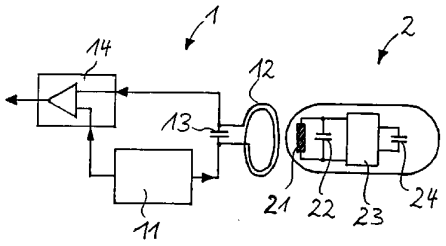
(72) **Inventeur(s) :** GRASSMANN NORBERT.

(73) **Titulaire(s) :**

(74) **Mandataire :** CABINET DE BOISSE.

(54) PROCEDE DE COMMANDE D'UN SYSTEME ANTIVOL, NOTAMMENT POUR VEHICULE AUTOMOBILE, ET SYSTEME ANTIVOL COMMANDE PAR UN TEL PROCEDE.

(57) Une serrure (1) émet un nombre aléatoire à destination d'une clé (2) . Celle-ci applique un algorithme de chiffrement au nombre aléatoire et renvoie un mot de code à la serrure (1). Dans la serrure, le mot de code est comparé à un mot de code de coupure, ce dernier étant engendré en appliquant le même algorithme de chiffrement au nombre aléatoire. Un signal de libération n'est engendré que s'il y a correspondance entre seulement une partie des bits du mot de code de consigne et du mot de code reçu.



FR 2 743 386 - A1

La présente invention concerne un procédé de commande d'un système antivol, notamment pour véhicule automobile, et un système antivol commandé par un tel procédé.

Un système antivol connu (EP 0 257 376 A1) comprend une clé et une serrure. Lorsqu'on la manoeuvre, la clé émet un signal codé qui est comparé dans la serrure à un signal codé de consigne. Si le signal codé ne correspond pas au signal codé de consigne, il est examiné, dans un premier domaine d'interception, s'il existe dans ce dernier un signal codé de consigne identique. Si, même dans ce premier domaine d'interception, il n'existe pas de correspondance, deux signaux codés successifs doivent alors correspondre à deux signaux codés de consigne successifs.

Dans ce système antivol, il doit se présenter une identité complète entre le signal codé transmis et le signal codé de consigne calculé dans la serrure. En cas de perturbations de transmission qui faussent en partie le signal codé, les portières ne peuvent pas être déverrouillées ou il convient de procéder à une nouvelle tentative.

L'invention a pour but de fournir un système antivol qui permette un verrouillage ou déverrouillage sûr ou une libération sûre du dispositif de blocage de conduite, même en cas de perturbations de transmission.

Conformément à l'invention, ce but est atteint au moyen d'un procédé de commande d'un système antivol, notamment pour véhicule automobile, comprenant une serrure et une clé, caractérisé par les opérations suivantes :

- un premier mot codé est produit dans la serrure et est émis à destination de la clé par un émetteur associé à la serrure,
- dans la clé, un second mot codé est produit à partir du premier mot codé et au moyen d'un algorithme mathématique rangé en mémoire dans la clé,

- le second mot codé est émis à destination de la serrure par un émetteur associé à la clé,

- le second mot codé est envoyé à une unité de comparaison associée à la serrure,

- un mot codé de consigne est produit dans une unité de calcul associée à la serrure, à partir du premier mot codé et d'un algorithme mathématique qui est identique à l'algorithme contenu dans la clé et il est envoyé aussi à l'unité de comparaison et

- le second mot codé reçu est comparé dans l'unité de comparaison au mot codé de consigne et un signal de libération est produit lorsqu'au moins une partie du mot codé correspond à au moins une partie du mot codé de consigne.

Le même but est atteint, conformément à l'invention, au moyen d'un système antivol, notamment pour véhicule automobile, comprenant une clé et une serrure, qui est commandé par un procédé tel que défini ci-dessus.

Suivant des développements avantageux du procédé conforme à l'invention, il peut être prévu :

- que l'algorithme mathématique soit un algorithme de chiffrement,

- que le mot codé de consigne et le second mot codé reçu soient comparés l'un à l'autre bit par bit et que le signal de libération soit produit lorsqu'au moins un nombre minimal de bits correspondent,

- que le mot codé de consigne et le second mot codé reçu soient comparés l'un à l'autre par groupes de plusieurs bits pour chacun et que le signal de libération soit produit chaque fois qu'au moins tous les bits sauf un correspondent à ceux du mot codé de consigne.

Suivant un développement avantageux du dispositif antivol conforme à l'invention, il peut être prévu que l'émetteur associé à la serrure et l'émetteur associé à la clé soient réalisés sous forme de bobines, les mots codés faisant l'objet d'une transmission par

transformation, dans un sens et dans l'autre, entre les bobines.

Un exemple avantageux de mise en oeuvre de l'invention est exposé ci-après en détail en regard des dessins schématiques. On voit :

à la figure 1, un schéma-bloc simplifié du système antivol conforme à l'invention,

à la figure 2, des mots codés du système antivol et,

à la figure 3, un schéma de déroulement d'un procédé de commande du système antivol.

Un système antivol conforme à l'invention comprend une serrure 1 (figure 1) et une clé 2. Il est prévu, disposée dans la serrure 1, une unité de calcul 11 qui produit d'abord un nombre aléatoire (voir aussi figure 3). Au moyen d'une unité émettrice et réceptrice qui comprend un circuit oscillant comportant une bobine 12 et un condensateur 13, le nombre aléatoire est transmis à la clé 2 lorsque cette clé 2 est située au voisinage direct de la serrure 1.

Il est aussi prévu, dans la clé 2, une unité émettrice et réceptrice qui comprend un circuit oscillant comportant une bobine 21 et un condensateur 22 et au moyen de laquelle le nombre aléatoire est capté. Le nombre aléatoire est appliqué à une unité de calcul 23, associée à la clé, qui applique plusieurs fois un algorithme mathématique au nombre aléatoire et à un nombre secret rangé en mémoire dans la clé 2 et ne pouvant pas être lu.

Cela pemet de produire un mot codé qui est retransmis à la serrure 1 par l'intermédiaire des bobines 12, 21 couplées l'une à l'autre d'une manière inductive.

Dans l'unité de calcul 11 de la serrure 1, le même algorithme mathématique que dans la clé 2 est appliqué au nombre aléatoire et au nombre secret rangé aussi en mémoire dans la serrure 1. Il est ainsi produit, dans la serrure 1, un mot codé de consigne qui

est envoyé à un comparateur 14. Le mot codé reçu par la clé 2 est envoyé aussi au comparateur 14. Le mot codé et le mot codé de consigne sont comparés l'un à l'autre dans le comparateur 14 et, lorsqu'au moins une grande partie du mot codé et une grande partie du mot codé de consigne correspondent l'une à l'autre, il est produit un signal de libération qui verrouille ou déverrouille les portières du véhicule ou libère le dispositif de blocage de conduite.

Les mots codés, le nombre aléatoire et le nombre secret sont des signaux binaires comportant chacun un nombre préfixé de bits. C'est ainsi par exemple que le nombre aléatoire peut avoir une longueur de 6 octets, c'est-à-dire de 48 bits. Un nombre secret présentant une longueur de 16 octets peut être rangé en mémoire dans la clé 2. Comme exemple le plus simple d'un algorithme mathématique, c'est par exemple un calcul logique EXOR qui peut être appliqué plusieurs fois au nombre aléatoire et au nombre secret, de sorte qu'un mot codé d'une longueur de 6 octets peut par exemple être produit. Il en est de même dans la serrure 1 dans laquelle un mot codé de consigne d'une longueur de 6 octets est produit à partir du nombre aléatoire, du nombre secret et de l'algorithme mathématique.

Le mot codé reçu et le mot codé de consigne produit sont comparés l'un à l'autre bit par bit dans le comparateur. Du fait de perturbations de transmission qui sont dues à des perturbations d'ondes électromagnétiques dans l'environnement du système antivol ou à des émetteurs parasites extérieurs, il peut se faire que la transmission du mot codé soit perturbée. De ce fait, quelques bits du mot codé peuvent être modifiés d'une manière non intentionnelle. Les effets d'une telle perturbation sont par exemple représentés à la figure 2. Sur celle-ci, le mot codé est représenté à la partie supérieure et, du fait d'une perturbation, il diffère en deux bits du mot codé de consigne représenté à la partie inférieure.

Or, dans le système antivol conforme à l'invention, il est désormais permis que le mot codé reçu et le mot codé de consigne produit diffèrent d'un nombre maximal préfixé de bits erronés, par exemple de 10 bits. Ce n'est que si les deux mots codés diffèrent d'un nombre de bits erronés supérieur au nombre maximal que le signal de libération n'est plus produit.

Le système antivol peut aussi être conçu de façon que, sur un octet (c'est-à-dire sur 8 bits) ou sur 4 bits, un seul bit erroné soit autorisé. Dans ce cas, un mot codé conforme à la figure 2 ne conduirait pas à un signal de libération, étant donné que, dans le second octet, deux bits sont d'emblée erronés. Plus le nombre de bits erronés qui est autorisé en tout est faible, plus la sécurité du système antivol est élevée. Toutefois, la sensibilité vis-à-vis de perturbations extérieures croît en même temps.

Avec ce système antivol, il est possible que le dispositif de blocage de conduite puisse être libéré lors du démarrage du véhicule automobile, même dans le cas de perturbations d'ondes électromagnétiques qui ne sont pas trop importantes. Une seconde tentative de démarrage n'est alors plus nécessaire. De même, les portières peuvent être verrouillées ou déverrouillées d'une manière sûre.

La fonction d'un dispositif de blocage de conduite peut alors être réalisée dans un dispositif de commande de moteur. Ce n'est que lorsque le signal de libération qui a été autorisé parvient au dispositif de commande de moteur qu'il est possible de faire démarrer le moteur et de conduire le véhicule automobile. Le dispositif de commande de moteur peut aussi produire le nombre aléatoire et l'envoyer à la serrure 1.

Le mot codé peut comporter aussi une partie propre au véhicule qui est accrochée au mot codé avant l'émission, ou bien à laquelle l'algorithme mathématique est aussi appliqué. Le mot codé de consigne doit alors comporter aussi une telle partie propre au véhicule.

L'unité de calcul située dans la clé 2 et dans la serrure 1 peut aussi être réalisée sous forme d'un transpondeur de chiffrement. Dans un tel transpondeur, c'est un algorithme mathématique déterminé qui se déroule, cet algorithme mathématique étant appliqué plusieurs fois au nombre aléatoire et au nombre secret. L'algorithme ne peut pas être lu de l'extérieur.

L'énergie prévue pour la clé 2 peut être émise à destination de cette clé 2 avec le nombre aléatoire et faire l'objet d'un stockage provisoire dans un accumulateur d'énergie 24. Toutefois, la clé 2 peut comporter aussi sa propre pile ou un accumulateur rechargeable.

Dans le système antivol, par "clé 2", on désigne un dispositif qui reçoit un mot aléatoire, soumet ce dernier à un traitement et renvoie un mot codé à la serrure 1. Ce dispositif peut être disposé sur une clé mécanique classique 2, sur une carte de la taille d'une carte de crédit ou sur un dispositif mécanique fonctionnellement équivalent.

Par "serrure 1", on désigne un dispositif qui émet le mot aléatoire et reçoit le mot codé. Le mot codé reçu est comparé à un mot codé de consigne produit dans la serrure 1. Dans le cas où le mot codé est juste, la serrure 1 produit un signal de libération qui est émis à destination d'un ensemble de sécurité, tel que le dispositif de blocage de conduite, ou des verrouillages de portières.

Le procédé de commande d'un système antivol conforme à l'invention peut être utilisé partout où on a jusqu'à présent utilisé des procédés de chiffrement pour l'identification ou l'authentification. C'est ainsi qu'on peut par exemple l'utiliser aussi pour des cartes à puce avec chiffrement, des cartes de téléphone, des cartes de crédit pour distributeur automatique d'argent, etc..

Le système antivol est utilisé avantageusement dans des véhicules automobiles, la clé 2 étant une clé

de contact qui reçoit alors le nombre aléatoire lorsqu'on enfonce la clé de contact dans la serrure de contact et qu'on la fait tourner dans cette serrure de contact pour faire démarrer le moteur.

REVENDICATIONS

1. Procédé de commande d'un système antivol, notamment pour véhicule automobile, comprenant une serrure (1) et une clé (2), caractérisé par les opérations suivantes :

- un premier mot codé est produit dans la serrure (1) et est émis à destination de la clé (2) par un émetteur (12) associé à la serrure,

- dans la clé (2), un second mot codé est produit à partir du premier mot codé et au moyen d'un algorithme mathématique rangé en mémoire dans la clé,

- le second mot codé est émis à destination de la serrure (12) par un émetteur (21) associé à la clé,

- le second mot codé est envoyé à une unité de comparaison (14) associée à la serrure,

- un mot codé de consigne est produit dans une unité de calcul (11) associée à la serrure, à partir du premier mot codé et d'un algorithme mathématique qui est identique à l'algorithme contenu dans la clé (2) et il est envoyé aussi à l'unité de comparaison (14) et

- le second mot codé reçu est comparé dans l'unité de comparaison (14) au mot codé de consigne et un signal de libération est produit lorsqu'au moins une partie du mot codé correspond à au moins une partie du mot codé de consigne.

2. Procédé selon la revendication 1, caractérisé en ce que l'algorithme mathématique est un algorithme de chiffrement.

3. Procédé selon la revendication 1, caractérisé en ce que le mot codé de consigne et le second mot codé reçu sont comparés l'un à l'autre bit par bit et en ce que le signal de libération est produit lorsqu'au moins un nombre minimal de bits correspondent.

4. Procédé selon la revendication 1, caractérisé en ce que le mot codé de consigne et le second mot codé reçu sont comparés l'un à l'autre par

groupes de plusieurs bits pour chacun et en ce que le signal de libération est produit chaque fois qu'au moins tous les bits sauf un correspondent avec ceux du mot codé de consigne.

5. Système antivol, notamment pour véhicule automobile, comprenant une clé (1) et une serrure (2), qui est commandé par un procédé selon la revendication 1.

6. Système antivol selon la revendication 5, caractérisé en ce que l'émetteur associé à la serrure et l'émetteur associé à la clé sont réalisés sous forme de bobines (12, 21), les mots codés faisant l'objet d'une transmission par transformation, dans un sens et dans l'autre, entre les bobines.

2743386

FIG 1

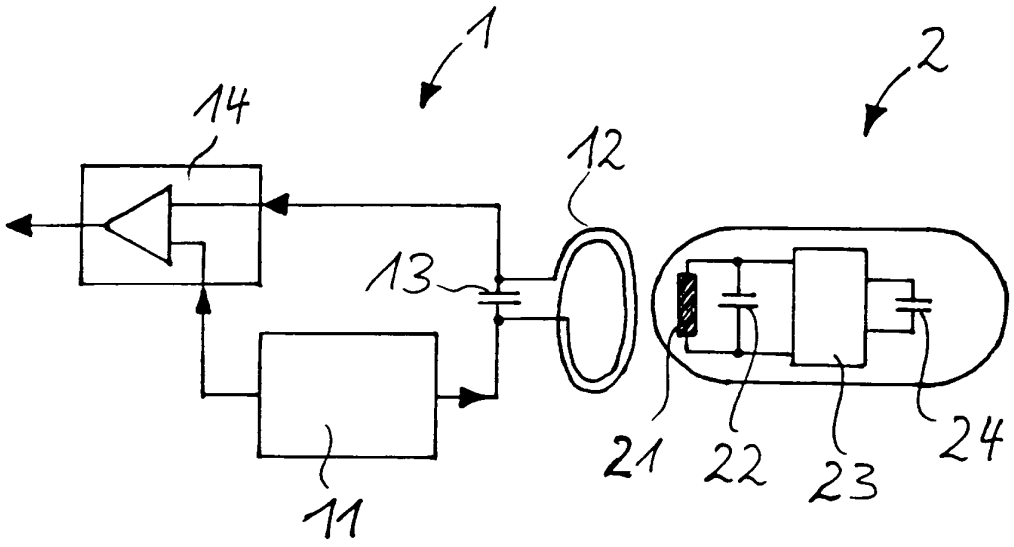


FIG 2

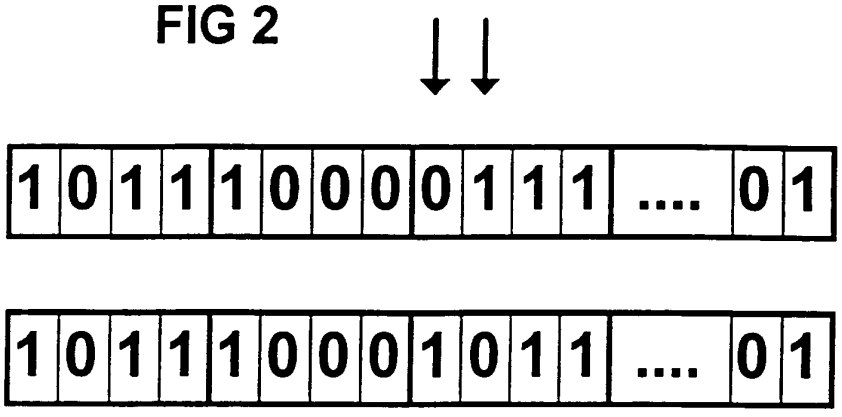
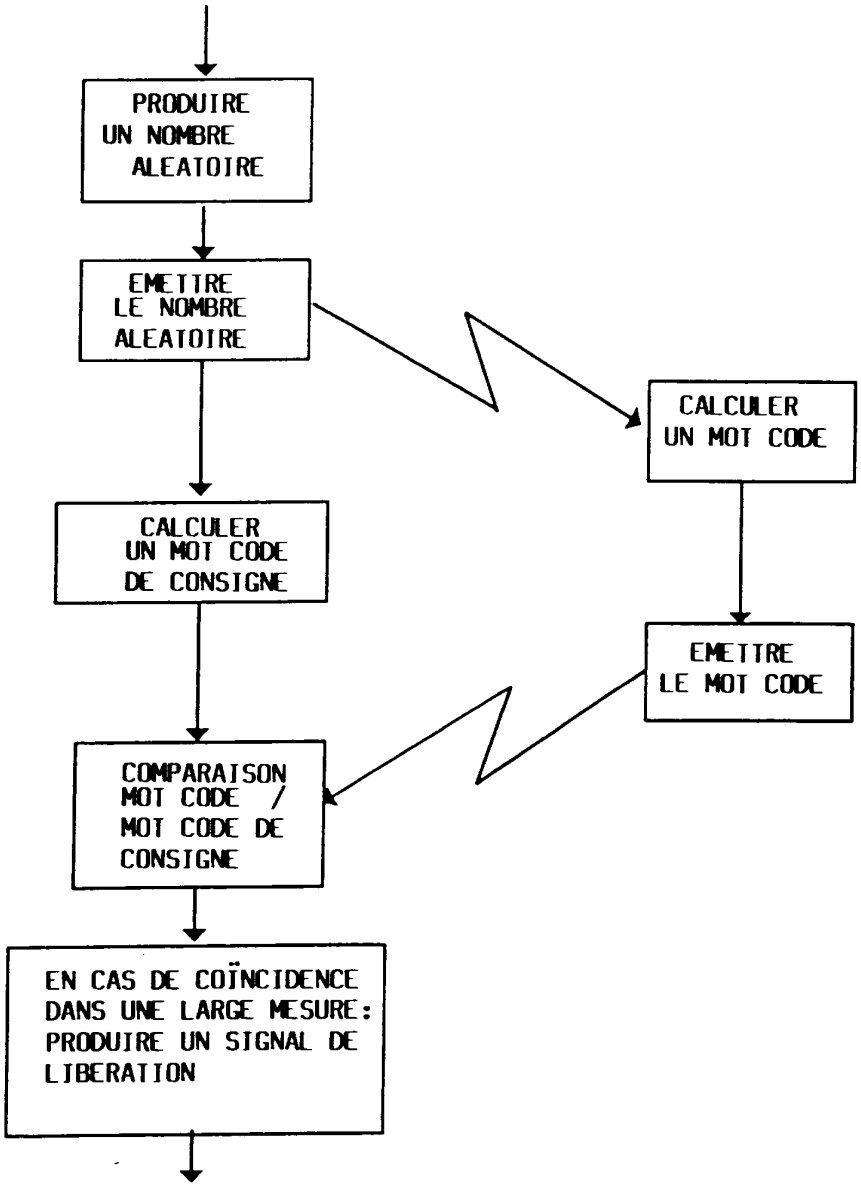


FIG 3


PRODUIRE UN NOMBRE ALEATOIRE
EMETTRE LE NOMBRE ALEATOIRE
CALCULER UN MOT CODE
CALCULER UN MOT CODE DE CONSIGNE
EMETTRE LE MOT CODE
COMPARAISON MOT CODE / MOT CODE DE CONSIGNE
EN CAS DE COÏNCIDENCE DANS UNE LARGE MESURE: PRODUIRE UN SIGNAL DE LIBERATION