(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 793 050**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **99 05570**

(51) Int Cl[7] : **G 06 F 12/14**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.04.99.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 03.11.00 Bulletin 00/44.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

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

(71) **Demandeur(s) :** *FINGERPRINT Société à responsabilité limitée* — FR.

(72) **Inventeur(s) :** CUENOD JEAN CHRISTOPHE et SGRO GILLES.

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

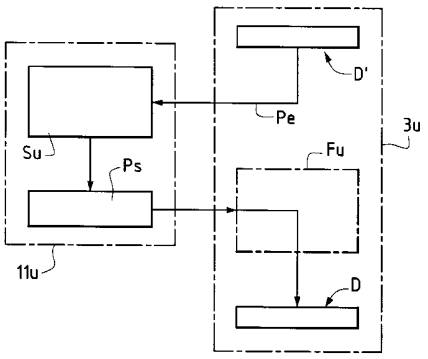
(74) **Mandataire(s) :** BEAU DE LOMENIE.

(54) PROCEDE POUR SECURISER UN LOGICIEL D'UTILISATION A PARTIR D'UNE UNITE DE TRAITEMENT ET DE MEMORISATION D'UN SECRET ET SYSTEME EN FAISANT APPLICATION.

(57) . L'invention concerne un procédé pour sécuriser un logiciel d'utilisation à partir d'une unité de traitement et de mémorisation d'utilisation (11_u) comportant au moins un secret d'utilisation (S_u).

. Selon l'invention, le procédé consiste:

- à mettre à disposition d'un utilisateur, un logiciel d'utilisation et des données modifiées (D'),
- et dans une phase de mise en oeuvre du logiciel d'utilisation avec les données modifiées (D') associées, à permettre à l'utilisateur possédant l'unité d'utilisation (11_u), de revenir aux données originales (D) à partir des données modifiées (D').



FR 2 793 050 - A1

La présente invention concerne le domaine technique des systèmes de traitement de données au sens général et elle vise, plus précisément, les moyens pour sécuriser l'utilisation d'un logiciel fonctionnant sur lesdits systèmes de traitement de données.

L'objet de l'invention vise, plus particulièrement, les moyens pour sécuriser un logiciel d'utilisation à partir d'une unité de traitement et de mémorisation d'un secret, désignée communément par carte à puce.

Dans le domaine technique ci-dessus, le principal inconvénient concerne l'emploi non autorisé de logiciels par des utilisateurs n'ayant pas acquitté des droits de licence. Cette utilisation illicite de logiciels cause un préjudice manifeste pour les éditeurs et les distributeurs de logiciels. Pour éviter de telles copies illicites, il a été proposé dans l'état de la technique diverses solutions pour protéger des logiciels. Ainsi, il est connu une solution de sécurisation consistant à mettre en oeuvre un système matériel de protection, tel qu'un élément physique appelé clé de protection ou "dongle" en terminologie anglo-saxonne. Une telle clé de protection devrait garantir à l'éditeur du logiciel l'exécution du logiciel uniquement en présence de la clé.

Or, il doit être constaté qu'une telle solution est inefficace car elle présente l'inconvénient d'être facilement contournable. Une personne mal intentionnée ou pirate peut, à l'aide d'outils spécialisés, tels que des désassembleurs, supprimer les instructions de contrôle. Il devient alors possible de réaliser des copies illicites correspondant à des versions modifiées des logiciels n'ayant plus aucune protection. De plus, cette solution ne peut pas être généralisée à tous les logiciels, dans la mesure où il est difficile de connecter plus de deux clés de protection sur une même machine.

L'objet de l'invention vise justement à remédier aux inconvénients énoncés ci-dessus en proposant un procédé pour sécuriser un logiciel d'utilisation à partir d'une unité de traitement et de mémorisation d'un secret, dans la mesure où la présence d'une telle unité est indispensable au fonctionnement correct du logiciel.

Pour atteindre un tel objectif, le procédé selon l'invention vise à sécuriser un logiciel d'utilisation à partir d'au moins une unité de traitement et de mémorisation d'au moins un secret d'utilisation, le logiciel fonctionnant sur un système de traitement de données d'utilisation. Conformément à l'objet de l'invention, le procédé consiste :

- à mettre à disposition d'un utilisateur, un logiciel d'utilisation et des données modifiées obtenues à partir d'un secret de génération et d'au moins une partie de données originales associées au logiciel d'utilisation,
- et dans une phase de mise en oeuvre du logiciel d'utilisation avec les données modifiées associées :
  - à choisir un paramètre d'entrée constitué par au moins une partie des données modifiées,
  - à transférer le paramètre d'entrée du système d'utilisation à l'unité d'utilisation,
  - à assurer la détermination par ladite unité d'utilisation, d'au moins un paramètre de sortie à partir du secret d'utilisation et du paramètre d'entrée,
  - à transférer le paramètre de sortie de l'unité d'utilisation au système d'utilisation,
  - et à mettre en oeuvre au moins une fonction d'utilisation utilisant au moins en partie, le paramètre de sortie, en vue d'obtenir les données originales.

Le procédé selon l'invention permet ainsi de sécuriser un logiciel d'utilisation par la mise en oeuvre d'une unité de traitement et de mémorisation d'un secret d'utilisation, qui présente la particularité de conserver l'information confidentielle même après plusieurs utilisations du secret. Il apparaît ainsi que toute version dérivée du logiciel tentant de fonctionner sans ladite unité "ad hoc", est incapable de se servir des données produites par un logiciel de génération, dans la mesure où le secret contenu dans l'unité de traitement et de mémorisation est hors d'atteinte. L'utilisation d'un secret de génération permet de modifier de manière non prédictible le format de stockage des données, de sorte que l'utilisation des données modifiées ne permet pas d'obtenir un fonctionnement correct du logiciel si l'utilisateur ne possède pas le secret d'utilisation. L'objet de l'invention trouve une application particulièrement avantageuse, notamment dans le cas de logiciels associés à la distribution fréquente de bibliothèques au sens général, dont le contenu constitue des données présentant un intérêt à être protégées, comme par exemple les encyclopédies ou les jeux.

Diverses autres caractéristiques ressortent de la description faite ci-dessous en référence aux dessins annexés qui montrent, à titre d'exemples non limitatifs, des formes de réalisation et de mise en oeuvre de l'objet de l'invention.

La **fig. 1** est un schéma illustrant un exemple de réalisation matérielle permettant la mise en oeuvre de l'objet de l'invention pendant une première phase, à savoir de génération de données modifiées.

La **fig. 2** est un schéma illustrant un exemple de réalisation matérielle permettant la mise en oeuvre de l'objet de l'invention pendant une deuxième phase, à savoir de mise en oeuvre du logiciel d'utilisation avec ses données modifiées.

Les **fig. 3** à **6** sont des schémas de principe d'utilisation de données modifiées associées à un logiciel, selon diverses variantes de réalisation.

Conformément à l'objet de l'invention, le procédé selon l'invention comporte une première étape ou phase pendant laquelle des données modifiées sont générées à partir de données originales devant être protégées et associées à un logiciel d'utilisation. Le procédé selon l'invention comporte une deuxième étape ou phase au cours de laquelle est mis en oeuvre le logiciel d'utilisation avec les données modifiées.

La **fig. 1** illustre un dispositif général $\mathbf{1}_g$ permettant de mettre en oeuvre la première phase du procédé conforme à l'invention. Ce dispositif de génération $\mathbf{1}_g$ est adapté pour mettre en oeuvre un logiciel de génération $\mathbf{2}_g$ de données modifiées dont la fonction apparaîtra plus clairement dans la suite de la description. Dans l'exemple de réalisation illustré, le dispositif de génération $\mathbf{1}_g$ comporte un système de traitement de données, dit de génération $\mathbf{3}_g$ de tous types connus en soi, appelé système de génération $\mathbf{3}_g$ dans la suite de la description. Dans l'exemple considéré, le système de génération $\mathbf{3}_g$ constitue un ordinateur mais il doit être considéré qu'un tel système de génération $\mathbf{3}_g$ peut faire partie intégrante de divers dispositifs, au sens général. Dans l'exemple considéré, le système de génération $\mathbf{3}_g$ comporte au moins un processeur $\mathbf{4}_g$, au moins une mémoire de travail $\mathbf{5}_g$, au moins un support de mémorisation de données $\mathbf{6}_g$ et au moins un circuit interface d'entrées-sorties $\mathbf{7}_g$. Classiquement, les divers composants du système de génération $\mathbf{3}_g$ sont reliés entre-eux par l'intermédiaire d'un bus de communication $\mathbf{8}_g$.

Selon une première variante de réalisation, le circuit interface $\mathbf{7}_g$ est relié à un lecteur $\mathbf{10}_g$ d'une unité $\mathbf{11}_g$ de traitement et de mémorisation, dite de génération, comportant au moins un secret de génération $\mathbf{S}_g$. Selon cet exemple, cette unité de génération $\mathbf{11}_g$ est destinée à être lue par le lecteur $\mathbf{10}_g$, mais il doit être considéré qu'une telle unité de génération $\mathbf{11}_g$ peut se présenter sous la forme d'une clé matérielle de tous types, connectée sur un circuit d'entrée/sortie, directement sur le bus de communication $\mathbf{8}_g$,

ou par tout autre moyen de communication, tel qu'une liaison radio, par exemple. D'une manière générale, l'unité de génération $\mathbf{11_g}$ comporte au moins un secret de génération $\mathbf{S_g}$ ou un dispositif de mémorisation d'une information codée, des moyens algorithmiques de traitement de données, et un système d'échange de données entre l'unité de génération $\mathbf{11_g}$ et le système génération $\mathbf{3_g}$. Classiquement, l'unité de génération $\mathbf{11_g}$ est réalisée par une carte à puce.

Selon une deuxième variante de réalisation, le secret de génération $\mathbf{S_g}$ est un paramètre du logiciel de génération $\mathbf{2_g}$.

Un tel dispositif de génération $\mathbf{1_g}$ permet d'exécuter la phase de création de données modifiées. Lors de cette phase, il est établi en relation du logiciel d'utilisation $\mathbf{2_u}$, des données dites originales **D** associées. Ces données originales **D**, qui sont destinées à être associées au logiciel d'utilisation $\mathbf{2_u}$ lors de la mise en oeuvre de ce dernier, constituent des données devant être protégées compte tenu de leur intérêt économique. Ces données originales **D** peuvent constituer, par exemple, une bibliothèque associée à un logiciel d'encyclopédie ou des scènes de jeux associées à un logiciel de jeu.

A partir d'au moins une partie de ces données originales **D**, le procédé assure la détermination de données modifiées **D'** en mettant en oeuvre un secret de génération $\mathbf{S_g}$. Ces données originales **D** et les données modifiées **D'** sont obtenues à partir d'un logiciel de génération $\mathbf{2_g}$ au sens général. Selon la première variante de réalisation, le secret de génération $\mathbf{S_g}$ peut être inclus dans une unité de traitement et de mémorisation, dite de génération $\mathbf{11_g}$. La mise en oeuvre de cette unité de génération $\mathbf{11_g}$ permet, lorsque le secret de génération $\mathbf{S_g}$ n'est pas connu, de rendre difficile, voire impossible, la déduction des données modifiées **D'** à partir des données originales **D**, même pour la personne ayant généré les données modifiées associées au logiciel. Selon la deuxième variante de réalisation, le secret de génération $\mathbf{S_g}$ peut être directement associé au logiciel de génération $\mathbf{2_g}$, de sorte que son caractère secret existe à l'exclusion du ou des développeurs du logiciel.

Après cette phase de codage ou de génération de données modifiées, les données modifiées **D'** sont fournies aux utilisateurs en association avec le logiciel d'utilisation $\mathbf{2_u}$. Ainsi, au terme d'une phase de codage, il est mis à disposition d'au moins un utilisateur, le logiciel d'utilisation $\mathbf{2_u}$ et des données modifiées **D'** obtenues à partir d'un secret de génération $\mathbf{S_g}$ et d'au moins une partie des données originales associées au logiciel

d'utilisation 2_u. Un tel logiciel d'utilisation avec ses données modifiées **D'**, peut alors être mis en oeuvre par au moins un utilisateur pendant une phase d'utilisation. Au cours de cette phase d'utilisation, chaque utilisateur pourvu d'un secret d'utilisation associé audit logiciel 2_u, est en mesure de modifier de façon inverse ou décoder les données modifiées **D'**, afin de retrouver et d'utiliser les données originales **D**. Il doit être compris que les données modifiées **D'** sont retraduites par le logiciel d'utilisation 2_u pour permettre de retrouver les données originales **D**, en présence du secret d'utilisation S_u.

La **fig. 2** illustre un dispositif d'utilisation 1_u permettant de mettre en oeuvre la deuxième phase du procédé conforme à l'invention. Dans l'exemple de réalisation illustré, le dispositif d'utilisation 1_u comporte un système de traitement de données, dit d'utilisation 3_u de tous types connus en soi, désigné par système d'utilisation 3_u dans la suite de la description. Dans l'exemple considéré, le système d'utilisation 3_u constitue un ordinateur mais il doit être noté qu'un tel système d'utilisation 3_u peut faire partie intégrante de diverses machines, dispositifs ou véhicules au sens général. Dans l'exemple considéré, le système d'utilisation 3_u comporte au moins un processeur 4_u, au moins une mémoire de travail 5_u, au moins un support de mémorisation de données 6_u et au moins un circuit interface d'entrées-sorties 7_u. Classiquement, les divers composants du système d'utilisation 3_u sont reliés entre-eux par l'intermédiaire d'un bus de communication 8_u. Le circuit interface 7_u est relié à un lecteur 10_u d'une unité de traitement et de mémorisation, dite d'utilisation 11_u, comportant au moins un secret d'utilisation S_u. Dans l'exemple illustré, cette unité 11_u, dite d'utilisation dans la suite de la description, est destinée à être lue par le lecteur 10_u, mais il doit être considéré qu'une telle unité d'utilisation 11_u peut se présenter sous la forme d'une clé matérielle de tous types, connectée sur un circuit d'entrée/sortie, directement sur le bus de communication 8_u, ou par tout autre moyen de communication, tel qu'une liaison radio, par exemple. D'une manière générale, l'unité d'utilisation 11_u comporte au moins un secret d'utilisation S_u ou un dispositif de mémorisation d'une information codée, des moyens algorithmiques de traitement de données, et un système d'échange de données entre l'unité d'utilisation 11_u et le système d'utilisation 3_u. Classiquement, l'unité d'utilisation 11_u est réalisée par une carte à puce.

La **fig. 3** illustre une première variante de réalisation du procédé conforme à l'invention permettant de traduire de façon inverse, les données modifiées **D'**, afin de

retrouver les données originales **D**, en mettant en oeuvre le dispositif d'utilisation 1_u. Le procédé consiste à choisir au moins un paramètre d'entrée P_e pour l'unité d'utilisation 11_u. Ce paramètre d'entrée P_e est constitué par au moins une partie des données modifiées **D'**. Le paramètre d'entrée P_e est transféré du système d'utilisation 3_u à l'unité d'utilisation 11_u. Cette unité d'utilisation 11_u assure la détermination d'au moins un paramètre de sortie P_s à partir d'au moins un secret d'utilisation S_u et du paramètre d'entrée P_e.

Il est à noter que le secret d'utilisation S_u peut être constitué soit par au moins une fonction secrète qui, à partir du paramètre d'entrée P_e, génère le paramètre de sortie P_s, soit par au moins une information secrète et au moins une fonction de conversion connue ou non, permettant de délivrer à partir du paramètre d'entrée P_e et de l'information secrète, le paramètre de sortie P_s. La mise en oeuvre de l'unité d'utilisation 11_u permet, lorsque le secret d'utilisation n'est pas connu, de rendre difficile, voire impossible, la déduction du paramètre de sortie P_s, à partir du paramètre d'entrée P_e.

L'unité d'utilisation 11_u assure ensuite le transfert du paramètre de sortie P_s au système d'utilisation 3_u. Un tel système d'utilisation 3_u assure la mise en oeuvre d'au moins une fonction d'utilisation F_u qui en utilisant au moins en partie le paramètre de sortie P_s, permet d'obtenir les données originales **D**.

Dans un exemple préféré de la variante de réalisation illustrée à la **fig. 3**, le paramètre d'entrée P_e est égal aux données modifiées **D'**, tandis que le paramètre de sortie P_s est égal aux données originales **D** recréées. Lors de la phase de génération des données, le secret de génération S_g assure une fonction de transformation inverse du secret d'utilisation S_u, c'est-à-dire que son paramètre d'entrée est égal aux données originales **D**, tandis que le paramètre de sortie de l'unité de génération est égal aux données modifiées **D'**.

Il apparaît ainsi que le détenteur d'une unité d'utilisation 11_u affectée à un logiciel d'utilisation 2_u déterminé peut retrouver et utiliser les données originales **D** associées audit logiciel. En effet, la mise en oeuvre du logiciel d'utilisation 2_u permet, en présence de l'unité d'utilisation 11_u "ad hoc", de traduire les données modifiées **D'** associées audit logiciel 2_u, en vue d'obtenir les données originales **D**. Par contre, un utilisateur ne possédant pas l'unité d'utilisation 11_u correspondante au logiciel d'utilisation 2_u peut utiliser ce dernier à l'exception des données originales **D** et au mieux avec les données modifiées.

De plus, l'efficacité du procédé selon l'invention est réelle, même si la fonction d'utilisation $\mathbf{F_u}$ est connue et si les paramètres d'entrée $\mathbf{P_e}$ et de sortie $\mathbf{P_s}$ sont observables et modifiables par une personne mal intentionnée en considérant, bien entendu, que le secret d'utilisation $\mathbf{S_u}$ est conservé. En effet, une telle personne est incapable de retrouver la modification des données **D'** en **D**.

Une personne mal intentionnée peut tenter de modifier le logiciel d'utilisation $\mathbf{2_u}$, de manière à ne plus avoir besoin de l'unité d'utilisation $\mathbf{11_u}$ correspondante. Pour ce faire, il convient de disposer, tout d'abord, de l'unité d'utilisation $\mathbf{11_u}$ "ad hoc". Ensuite, il est nécessaire que cette personne énumère l'ensemble des données modifiées **D'** pour soit établir une table de correspondance entre tous les paramètres d'entrée $\mathbf{P_e}$ et les paramètres de sortie $\mathbf{P_s}$, en vue de générer un pseudo-simulateur de l'unité d'utilisation $\mathbf{11_u}$, soit recréer l'ensemble des données originales **D** et établir un nouvelle distribution du logiciel d'utilisation $\mathbf{2'_u}$ incluant ces données originales recréées à la place des données modifiées, et permettant de s'affranchir de la phase de décodage ou de traduction en sens inverse des données modifiées. Cependant, une telle tâche est difficile en raison du grand nombre de données originales.

Dans l'exemple de réalisation illustré à la **fig. 3**, les données modifiées **D'** sont transférées totalement à l'unité d'utilisation $\mathbf{11_u}$. Pour améliorer la vitesse d'un tel dispositif, les **fig. 4** à **6** décrivent diverses variantes préférées de réalisation du procédé de sécurisation conforme à l'invention.

La **fig. 4** illustre une deuxième variante de réalisation pour la phase de mise en oeuvre du logiciel d'utilisation $\mathbf{2_u}$ avec les données modifiées. Selon cet exemple, les données modifiées **D'** sont décomposées en au moins une première partie $\mathbf{D'_1}$ et une deuxième partie $\mathbf{D'_2}$. Au moins la première partie $\mathbf{D'_1}$ des données modifiées est choisie comme paramètre d'entrée $\mathbf{P_e}$. Ce paramètre d'entrée $\mathbf{P_e}$ est transféré à l'unité d'utilisation $\mathbf{11_u}$ qui, à l'aide du secret d'utilisation $\mathbf{S_u}$, détermine un paramètre de sortie $\mathbf{P_s}$. L'unité d'utilisation $\mathbf{11_u}$ transfère le paramètre de sortie $\mathbf{P_s}$ au système d'utilisation $\mathbf{3_u}$. Le système d'utilisation $\mathbf{3_u}$ met en oeuvre une fonction d'utilisation $\mathbf{F_u}$ qui comporte une fonction de traduction inverse $\mathbf{T_i}$ qui en utilisant au moins en partie le paramètre de sortie $\mathbf{P_s}$ et la deuxième partie $\mathbf{D'_2}$ des données modifiées **D'**, permet de retrouver les données originales **D**.

Selon un exemple préféré de réalisation de la variante illustrée à la **fig. 4**, il est choisi comme première partie et deuxième partie des données modifiées **D'**, respectivement un nombre pseudo-aléatoire qui a été choisi lors de la phase de génération, et des données originales qui ont été modifiées lors de la phase de génération et appelées données originales modifiées $\mathbf{D'_2}$. Ce nombre pseudo-aléatoire est utilisé comme paramètre d'entrée $\mathbf{P_e}$ et transformé par le secret d'utilisation $\mathbf{S_u}$ pour obtenir le paramètre de sortie $\mathbf{P_s}$. La fonction de traduction inverse $\mathbf{T_i}$ permet, à partir du paramètre de sortie $\mathbf{P_s}$ et des données originales modifiées $\mathbf{D'_2}$, d'obtenir les données originales **D**. Dans la phase de génération correspondant à cet exemple préféré de réalisation, il est choisi un nombre pseudo-aléatoire comme paramètre d'entrée du secret de génération $\mathbf{S_g}$ qui délivre un paramètre de sortie de génération. Un tel paramètre de sortie est utilisé pour modifier par une fonction de traduction **T**, les données originales **D,** en vue d'obtenir les données originales modifiées. Ces données originales modifiées forment en association avec le nombre pseudo-aléatoire, les données modifiées **D'**. Bien entendu, la fonction de traduction inverse $\mathbf{T_i}$ est constituée par la fonction inverse de la fonction de traduction **T** ou par une combinaison de fonctions élémentaires équivalentes.

Selon la variante illustrée à la **fig. 4**, la modification des données originales **D** est totalement indépendante de celles-ci.

La **fig. 5** illustre une troisième variante de réalisation pour la phase de mise en oeuvre du logiciel d'utilisation $\mathbf{2_u}$ avec les données modifiées **D'**. Selon cette variante de réalisation, les données modifiées **D'** sont formées d'une première partie $\mathbf{D_1}$ et d'une deuxième partie $\mathbf{D'_2}$. Au moins une partie de cette première partie $\mathbf{D_1}$, qui correspond au paramètre d'entrée $\mathbf{P_e}$, est transférée à l'unité d'utilisation $\mathbf{11_u}$ qui détermine un paramètre de sortie $\mathbf{P_s}$ à l'aide du secret d'utilisation $\mathbf{S_u}$. Le paramètre de sortie $\mathbf{P_s}$ est transféré au système d'utilisation $\mathbf{3_u}$ qui met en oeuvre une fonction d'utilisation $\mathbf{F_u}$ comportant une fonction de traduction inverse $\mathbf{T_i}$ qui en utilisant au moins en partie, le paramètre de sortie $\mathbf{P_s}$ et la deuxième partie $\mathbf{D'_2}$ des données, permet de retrouver la deuxième partie originale $\mathbf{D_2}$ des données. La fonction d'utilisation $\mathbf{F_u}$ délivre également la première partie $\mathbf{D_1}$ des données originales qui associée à la deuxième partie $\mathbf{D_2}$, forment les données originales **D**.

Selon un exemple préféré de réalisation de la variante illustrée à la **fig. 5**, la première partie $\mathbf{D_1}$ correspond à une partie des données originales, tandis que la deuxième

partie $\mathbf{D'_2}$ correspond à l'autre partie des données originales qui ont été modifiées lors de la phase de génération et qui est appelée deuxième partie modifiée $\mathbf{D'_2}$ des données. La première partie $\mathbf{D_1}$ des données originales est transformée par le secret d'utilisation $\mathbf{S_u}$ pour obtenir le paramètre de sortie $\mathbf{P_s}$. Par ailleurs, la fonction d'utilisation $\mathbf{F_u}$ comporte une fonction de traduction inverse $\mathbf{T_i}$ qui, à partir du paramètre de sortie $\mathbf{P_s}$ et de la deuxième partie modifiée $\mathbf{D'_2}$ des données, permet de retrouver la deuxième partie $\mathbf{D_2}$ des données originales. De plus, la fonction d'utilisation $\mathbf{F_u}$ est adaptée pour délivrer aussi la première partie $\mathbf{D_1}$ des données originales qui, en combinaison avec la deuxième partie $\mathbf{D_2}$ des données originales, forment les données originales **D**. Dans la phase de génération correspondant à cet exemple préféré de réalisation, les données originales **D** sont décomposées en une première partie $\mathbf{D_1}$ et une deuxième partie $\mathbf{D_2}$. Au moins une partie de la première partie $\mathbf{D_1}$ est utilisée comme paramètre d'entrée du secret de génération $\mathbf{S_g}$ qui délivre un paramètre de sortie de génération. Au moins une partie du paramètre de sortie de génération est utilisée par une fonction de traduction faisant partie d'une fonction de génération pour traduire la deuxième partie $\mathbf{D_2}$ des données originales, en vue d'obtenir une deuxième partie modifiée $\mathbf{D'_2}$ des données. A la première partie $\mathbf{D_1}$ des données originales est associée cette deuxième partie modifiée $\mathbf{D'_2}$ des données, en vue de constituer les données modifiées **D'**.

Selon cette variante de réalisation, la modification des données originales **D** dépend uniquement de celles-ci.

La **fig. 6** illustre une quatrième variante de réalisation pour la phase de mise en oeuvre du logiciel d'utilisation $\mathbf{2_u}$ avec les données modifiées **D'**. Selon cet exemple, les données modifiées **D'** sont décomposées en une première partie $\mathbf{D_1}$, une deuxième partie $\mathbf{D'_2}$ et une troisième partie $\mathbf{D_3}$. Le paramètre d'entrée $\mathbf{P_e}$ est constitué par au moins une partie de la première partie $\mathbf{D_1}$ et de la troisième partie $\mathbf{D_3}$. Le paramètre d'entrée $\mathbf{P_e}$ est transféré à l'unité d'utilisation $\mathbf{11_u}$ qui détermine un paramètre de sortie $\mathbf{P_s}$ à l'aide d'un secret d'utilisation $\mathbf{S_u}$. Le paramètre de sortie $\mathbf{P_s}$ est transféré au système d'utilisation $\mathbf{3_u}$ qui met en oeuvre une fonction d'utilisation $\mathbf{F_u}$ comportant une fonction de traduction inverse $\mathbf{T_i}$ qui en utilisant au moins en partie le paramètre de sortie $\mathbf{P_s}$ et la deuxième partie $\mathbf{D'_2}$ des données, permet de retrouver la deuxième partie originales $\mathbf{D_2}$ des données. La fonction d'utilisation $\mathbf{F_u}$ délivre également la première partie $\mathbf{D_1}$ des données originales

qui, associée à la deuxième partie originale D_2 des données, forme les données originales **D**.

Selon un exemple préféré de réalisation de la variante illustrée à la **fig. 6**, la troisième partie D_3 correspond à un nombre pseudo-aléatoire qui a été choisi lors de la phase de génération, tandis que la première partie D_1 correspond à une partie des données originales **D**, alors que la deuxième partie D'_2 correspond à l'autre partie des données originales qui a été modifiée lors de la phase de génération et qui est appelée deuxième partie modifiée D'_2 des données. Au moins une partie de la première partie D_1 des données originales et au moins une partie du nombre pseudo-aléatoire forment le paramètre d'entrée P_e qui est transformé par le secret d'utilisation S_u pour obtenir le paramètre de sortie P_s. Par ailleurs, la fonction d'utilisation F_u comporte une fonction de traduction inverse T_i qui, à partir du paramètre de sortie P_s et de la deuxième partie modifiée D'_2 des données, permet de retrouver la deuxième partie D_2 des données originales. De plus, la fonction d'utilisation F_u est adaptée pour délivrer aussi la première partie D_1 des données qui, en combinaison avec la deuxième partie D_2 des données originales, forme les données originales **D**. Dans la phase de génération correspondant à cet exemple préféré de réalisation, les données originales **D** sont décomposées en une première partie D_1 et une deuxième partie D_2, tandis qu'un nombre pseudo-aléatoire est choisi comme troisième partie D_3. Au moins une partie de la première partie D_1des données et au moins une partie du nombre pseudo-aléatoire sont utilisées comme paramètres d'entrée du secret de génération S_g qui délivre un paramètre de sortie de génération. Au moins une partie du paramètre de sortie de génération est utilisée par une fonction de génération pour traduire la deuxième partie D_2 des données originales, en vue d'obtenir une deuxième partie modifiée D'_2 des données. Le nombre pseudo-aléatoire D_3 et la première partie D_1 des données originales sont associés à cette deuxième partie modifiée D'_2, afin de constituer les données modifiées **D'**.

Selon cette variante de réalisation, la modification des données originales **D** dépend simultanément de celles-ci et d'un nombre pseudo-aléatoire.

Selon une caractéristique préférée de réalisation attachée aux exemples décrits aux **fig. 5** et **6**, la première partie D_1 des données destinées à être transférées à l'unité d'utilisation 11_u, est traitée pour faciliter les opérations de traitement exécutées par l'unité

d'utilisation 11_u. Cette partie D_1 des données est ainsi fournie en entrée à au moins une fonction de traduction d'utilisation intermédiaire H_u, telle qu'une fonction non inversible, par exemple du type "one way hash", de manière à obtenir au moins un paramètre d'entrée intermédiaire P_{ei}. Ce paramètre d'entrée intermédiaire P_{ei} déterminé par le système d'utilisation 3_u, est éventuellement combiné avec la troisième partie D_3 pour former le paramètre d'entrée P_e. Ce paramètre d'entrée **Pe** est transféré à l'unité d'utilisation 11_u, de manière que cette dernière puisse assurer la détermination du paramètre de sortie P_s à partir du secret d'utilisation S_u et du paramètre d'entrée intermédiaire P_{ei}, et éventuellement de la troisième partie D_3.

Bien entendu, lors de la phase de génération des données modifiées **D'**, le système de génération met en oeuvre au moins une fonction de traduction intermédiaire de génération, de manière à obtenir au moins un paramètre d'entrée intermédiaire de génération.

Dans les exemples des **fig. 5** et **6**, il ressort que dans la phase d'utilisation, les données originales **D** sont obtenues au cours d'une étape de traitement mettant en oeuvre l'unité d'utilisation 11_u. Bien entendu, il peut être prévu de recommencer n fois cette étape de traitement pour augmenter la complexité du décodage des données. Ainsi, les opérations suivantes peuvent être recommencées autant de fois que nécessaires, à savoir :

- décomposer les données modifiées précédemment obtenues en au moins une première et une deuxième parties,
- déterminer au moins un paramètre de sortie à partir d'une fonction d'un ou de plusieurs secrets d'utilisation différents ou identiques de celui ou de ceux précédemment utilisés, et d'une partie des données,
- modifier au moins l'une des autres parties des données par une fonction de traduction identique ou différente de celle précédemment utilisée,
- et reconstituer des données après chaque phase de modification des données.

Selon cet exemple de réalisation, lors de la phase de génération des données modifiées, les opérations de génération des données sont conduites dans l'ordre inverse, un nombre de fois n identique au nombre d'étapes effectuées lors de la phase d'utilisation.

Selon une variante préférée de réalisation selon les fig. **5** et **6**, les données modifiées **D'** sont composées d'au moins deux parties D'_1, D'_2, par exemple de tailles sensiblement équivalentes. Dans une première étape de traitement, la deuxième partie D'_2

est utilisée comme paramètre d'entrée de l'unité d'utilisation 11_u, en vue de retrouver la première partie D_1 des données originales. Après une première étape de traitement, il est obtenu des données intermédiaires constituées par au moins la première partie D_1 des données originales et la deuxième partie modifiée D'_2 des données. Dans une deuxième étape de traitement, le rôle des parties D_1 et D'_2 est inversé. Ainsi, au moins la première partie D_1 des données est utilisée comme paramètre d'entrée de l'unité d'utilisation 11_u tandis que la deuxième partie modifiée D'_2 des données originales est modifiée par une fonction de traduction, en vue de retrouver la deuxième partie D_2 des données originales. Il s'ensuit que l'ensemble des données originales **D** sont obtenues après un décodage de la totalité des données originales. Bien entendu, lors de la phase de génération, des opérations inverses sont effectuées afin de coder l'ensemble des données originales **D**.

Selon une caractéristique préférée de mise en oeuvre de l'invention, les données modifiées **D'** sont écrites ou enregistrées sur le support 6_u de mémorisation de données, associé au système de traitement de données 3_u pour permettre l'utilisation des données modifiées **D'** lors de la phase d'utilisation du logiciel 2_u. Bien entendu, le support 6_u de mémorisation de données peut être constitué de toute manière connue, telle que par exemple un disque dur, une bande magnétique, un CD ROM, ou tout autre dispositif de mémorisation utilisé en vue du stockage ou d'une transmission de ces données.

Le procédé selon l'invention décrit ci-dessus peut être mis en oeuvre avec différentes fonctions d'utilisation F_u selon les objectifs souhaités par l'éditeur du logiciel protégé. Par exemple, la fonction d'utilisation F_u peut comporter une fonction de cryptage. Dans ce cas, les données traduites sont manifestement incompréhensibles. Selon un autre exemple de réalisation, la fonction d'utilisation F_u peut être une fonction de modification mineure pseudo-aléatoire des chiffres contenus dans les données originales. De cette manière, l'utilisateur d'un logiciel piraté $2'_u$ peut utiliser les données générées par la version originale du logiciel, mais celles-ci aboutissent à un fonctionnement erroné du logiciel d'utilisation $2'_u$.

L'invention n'est pas limitée aux exemples décrits et représentés, car diverses modifications peuvent y être apportées sans sortir de son cadre.

REVENDICATIONS :

1 - Procédé pour sécuriser un logiciel d'utilisation (2_u) à partir d'une unité de traitement et de mémorisation d'utilisation (11_u) comportant au moins un secret d'utilisation (S_u), ledit logiciel fonctionnant sur un système de traitement de données d'utilisation (3_u), caractérisé en ce qu'il consiste :

- à mettre à disposition d'un utilisateur, un logiciel d'utilisation (2_u) et des données modifiées (**D'**) obtenues à partir d'un secret de génération (S_g) et d'au moins une partie de données originales (**D**) associées au logiciel d'utilisation (**2u**),
- et dans une phase de mise en oeuvre du logiciel d'utilisation (2_u) avec les données modifiées (**D'**) associées :
  - ◊ à choisir un paramètre d'entrée (P_e) constitué par au moins une partie des données modifiées (**D'**),
  - ◊ à transférer le paramètre d'entrée (P_e) du système d'utilisation (3_u) à l'unité d'utilisation (11_u),
  - ◊ à assurer la détermination par ladite unité d'utilisation (11_u), d'au moins un paramètre de sortie (P_s) à partir du secret d'utilisation (S_u) et du paramètre d'entrée (P_e),
  - ◊ à transférer le paramètre de sortie (P_s) de l'unité d'utilisation (11_u) au système d'utilisation (3_u),
  - ◊ et à mettre en oeuvre au moins une fonction d'utilisation (F_u) utilisant au moins en partie, le paramètre de sortie (P_s), en vue d'obtenir les données originales (**D**).

2 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste, dans une phase de génération de données modifiées (**D'**) précédant la mise à disposition du logiciel d'utilisation (2_u) :

- à établir, à partir d'un logiciel de génération, des données dites originales (**D**) associées au logiciel d'utilisation (2_u),
- à assurer la détermination de données modifiées (**D'**) à partir d'un secret de génération (S_g) et d'au moins une partie des données originales (**D**).

3 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste :

- à choisir comme paramètre d'entrée (P_e), au moins en partie les données modifiées (**D'**),
- et à mettre en oeuvre une fonction d'utilisation (F_u) qui délivre les données originales (**D**) à partir du paramètre de sortie (P_s).

4 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste :

- à décomposer les données modifiées (**D'**) en au moins une première partie (D'_1) et une deuxième partie (D'_2),
- à choisir comme paramètre d'entrée (P_e), la première partie (D'_1) des données modifiées,
- et à mettre en oeuvre une fonction d'utilisation (F_u) qui délivre les données originales (**D**) en utilisant le paramètre de sortie (P_s) et la deuxième partie (D'_2) des données modifiées.

5 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste :

- à décomposer les données modifiées (**D'**) en au moins une première partie (D_1) et une deuxième partie (D'_2),
- à choisir comme paramètre d'entrée (P_e), la première partie (D_1) des données modifiées,
- et à mettre en oeuvre une fonction d'utilisation (F_u) qui délivre les données originales en utilisant le paramètre de sortie (P_s), la première partie (D_1) et la deuxième partie (D'_2) des données modifiées.

6 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste :

- à décomposer les données modifiées (**D'**) en au moins une première partie (D_1), une deuxième partie (D'_2) et une troisième partie (D_3),
- à déterminer le paramètre d'entrée (P_e) à partir d'au moins la première partie (D_1) et d'au moins la troisième partie (D_3),
- et à mettre en oeuvre une fonction d'utilisation (F_u) qui délivre les données originales (**D**) en utilisant le paramètre de sortie (P_s), la première partie (D_1) et la deuxième partie (D'_2) des données modifiées.

7 - Procédé selon la revendication 5 ou 6, caractérisé en ce qu'il consiste :

- à choisir comme paramètre d'entrée (P_e), un paramètre d'entrée intermédiaire (P_{ei}) défini par le système de traitement de données, à partir

d'une fonction de traduction intermédiaire (H_u) utilisant une partie des données modifiées,

- et à assurer la détermination du paramètre de sortie à partir du secret d'utilisation (S_u) et du paramètre d'entrée (P_e), constitué du paramètre d'entrée intermédiaire (P_{ei}) et éventuellement de la troisième partie des données (D_3).

8 - Procédé selon la revendication 1 ou 2, caractérisé en ce qu'il consiste à assurer détermination de données modifiées (**D'**) à partir d'un secret de génération (S_g) contenu dans une unité de traitement et de mémorisation de génération (11_g).

9 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste à assurer la détermination de données modifiées (**D'**) à partir d'un secret de génération (S_g) associé au logiciel de génération (2_g).

10 - Procédé selon la revendication 5 ou 6, caractérisé en ce qu'il consiste à recommencer n fois (avec $n \geq 1$), les opérations :

- de décomposition des données modifiées précédemment obtenues en au moins une première et deuxième parties,
- de détermination d'au moins un paramètre de sortie à partir d'une fonction d'un ou de plusieurs secrets d'utilisation différents ou identiques de ceux précédemment utilisés, et d'une partie des données,
- de modification d'au moins l'une des autres parties des données par une fonction de traduction identique ou différente de celle précédemment utilisée,
- et de reconstitution des données après chaque phase de modification des données.

11 - Procédé selon la revendication 10, caractérisé en ce qu'il consiste, dans la phase d'utilisation :

- dans une première étape de traitement :
  - à décomposer les données modifiées (**D'**) en au moins une première partie (D'_1) et une deuxième partie (D'_2),

- à utiliser au moins en partie, la deuxième partie ($\mathbf{D'_2}$) comme paramètre d'entrée de l'unité de d'utilisation ($\mathbf{11_u}$), en vue de retrouver la première partie ($\mathbf{D_1}$) des données originales,
- et à constituer des données intermédiaires composées par au moins la première partie ($\mathbf{D_1}$) des données originales et la deuxième partie modifiée ($\mathbf{D'_2}$) des données,

– et dans une deuxième étape de traitement :

- à utiliser, au moins en partie, la première partie ($\mathbf{D_1}$) des données, comme paramètre d'entrée de l'unité d'utilisation ($\mathbf{11_u}$), en vue de retrouver la deuxième partie ($\mathbf{D_2}$) des données originales,
- et à reconstituer les données originales (**D**) par la première partie ($\mathbf{D_1}$) et la deuxième partie ($\mathbf{D_2}$) des données.

12 - Procédé selon la revendication 10 ou 11, caractérisé en ce qu'il consiste à conduire n fois dans l'ordre inverse (avec $n \geq 1$), les opérations de traduction des données originales (**D**) pour obtenir les données modifiées (**D'**).

13 - Procédé selon la revendication 1, caractérisé en ce qu'il consiste à écrire les données modifiées (**D'**) sur un support (**6**) de mémorisation de données, associé au système d'utilisation ($\mathbf{3_u}$) pour permettre l'utilisation des données modifiées (**D'**) lors d'une phase d'utilisation du logiciel ($\mathbf{2_u}$).

14 - Dispositif pour sécuriser un logiciel d'utilisation ($\mathbf{2_u}$) à partir d'une unité de traitement et de mémorisation d'utilisation ($\mathbf{11_u}$) comportant au moins un secret d'utilisation ($\mathbf{S_u}$), ledit logiciel fonctionnant sur un système de traitement de données dit d'utilisation ($\mathbf{3_u}$), caractérisé en ce qu'il comporte :

– un logiciel d'utilisation ($\mathbf{2_u}$) et des données modifiées (**D'**) obtenues à partir d'un secret de génération ($\mathbf{S_g}$) et d'au moins une partie des données originales (**D**),

– et dans une phase de mise en oeuvre du logiciel d'utilisation ($\mathbf{2_u}$) avec les données modifiées (**D'**) :

◊ un système de traitement de données, dit d'utilisation ($\mathbf{3_u}$) comportant :

- des moyens permettant de déterminer un paramètre d'entrée ($\mathbf{P_e}$) constitué par au moins une partie des données modifiées (**D'**),

- des moyens de transfert du paramètre d'entrée ($\mathbf{P_e}$) du système d'utilisation ($\mathbf{3_u}$) à l'unité d'utilisation ($\mathbf{11_u}$),

◊ et une unité d'utilisation ($\mathbf{11_u}$) comportant :

- des moyens assurant la détermination d'au moins un paramètre de sortie ($\mathbf{P_s}$) à partir du secret d'utilisation ($\mathbf{S_u}$) et du paramètre d'entrée ($\mathbf{P_e}$),
- des moyens de transfert du paramètre de sortie ($\mathbf{P_s}$) de ladite unité d'utilisation ($\mathbf{11_u}$) au système d'utilisation ($\mathbf{3_u}$) qui met en oeuvre au moins une fonction d'utilisation ($\mathbf{F_u}$) utilisant au moins en partie, le paramètre de sortie ($\mathbf{P_s}$), en vue d'obtenir les données originales.

15 - Dispositif selon la revendication 14, caractérisé en ce qu'il comporte, dans la phase de génération de données modifiées, une unité de génération ($\mathbf{11_g}$) contenant un secret de génération permettant d'assurer la détermination de données modifiées (**D'**).

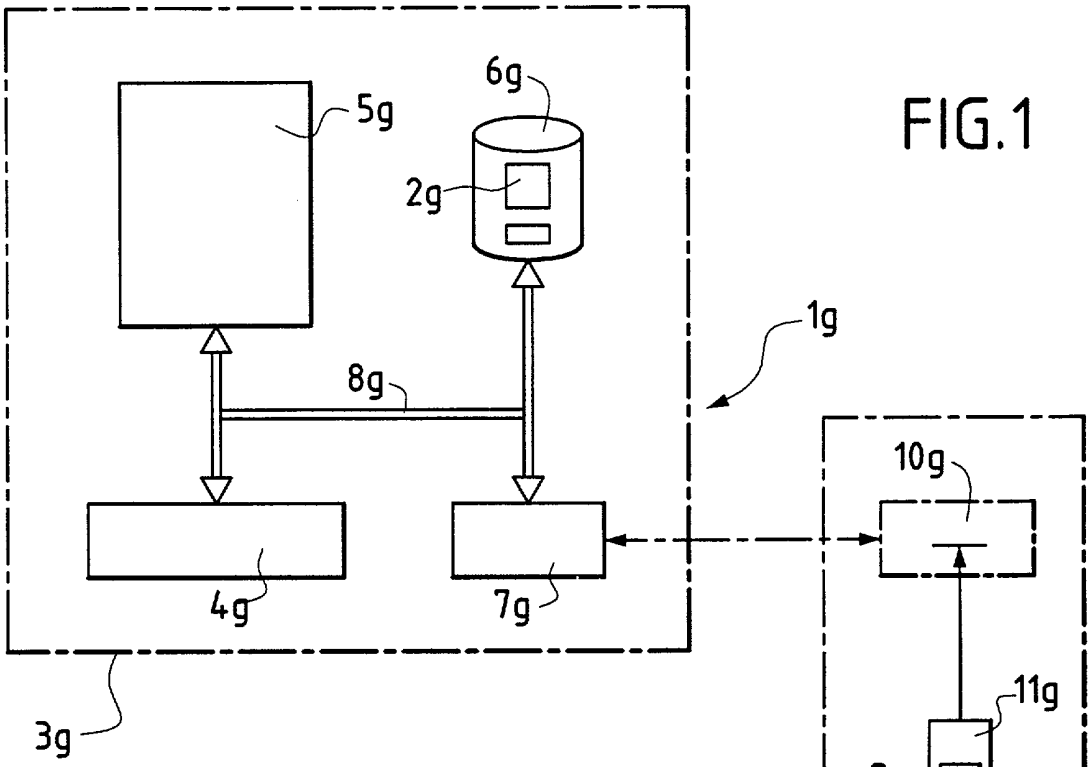


FIG.1

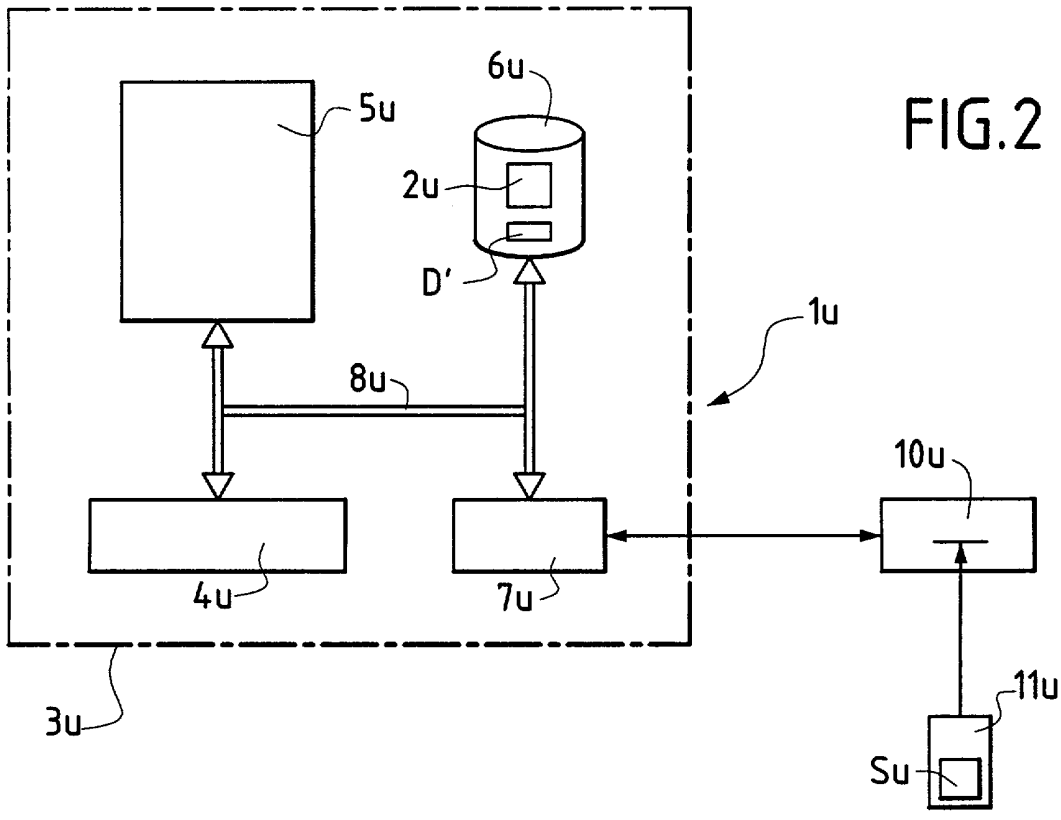


FIG.2

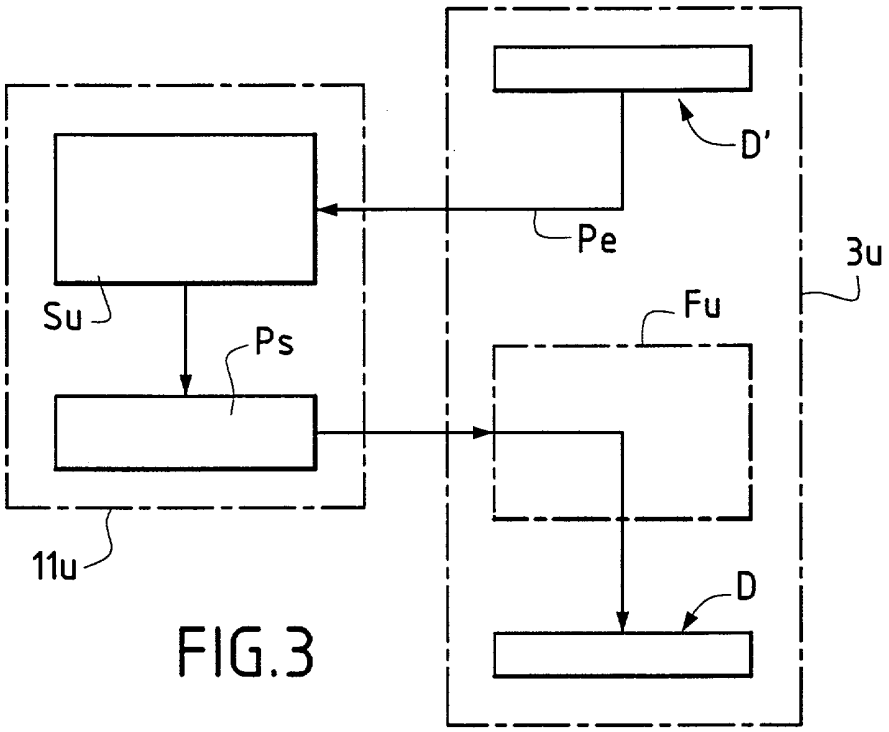


FIG.3

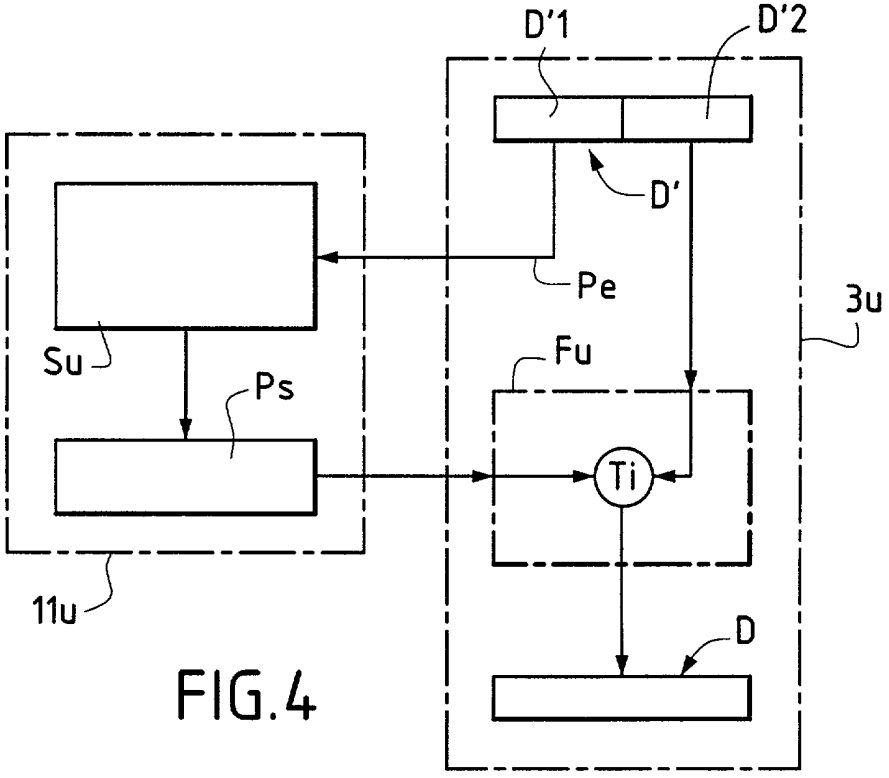


FIG.4

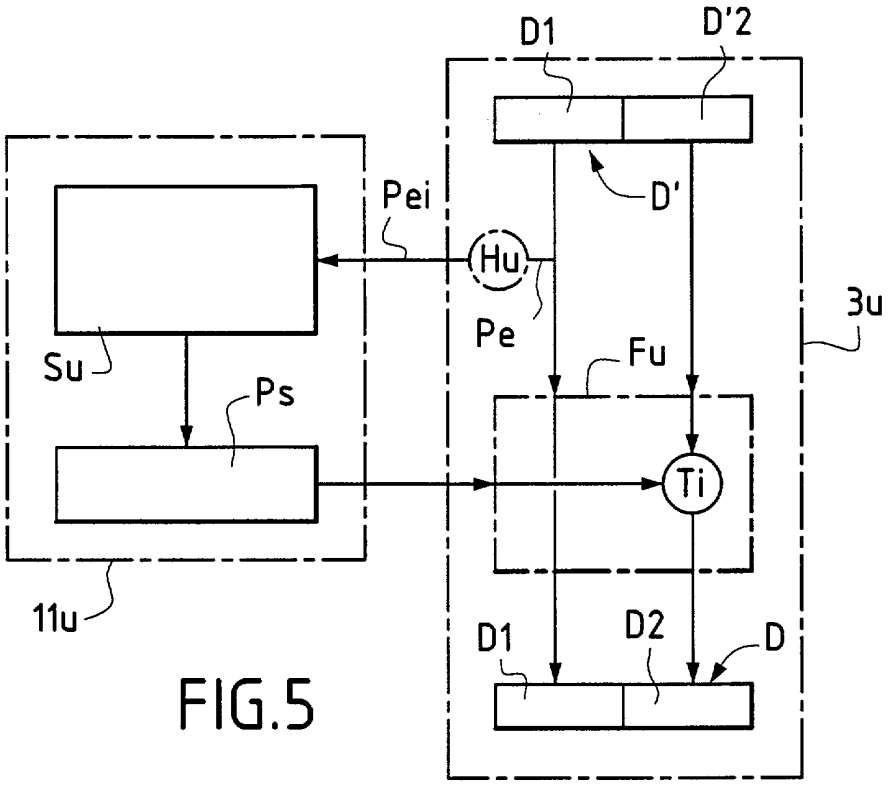

D1
D'2
D'
Pei
Hu
Pe
3u
Su
Ps
Fu
Ti
11u
D1
D2
D

FIG.5

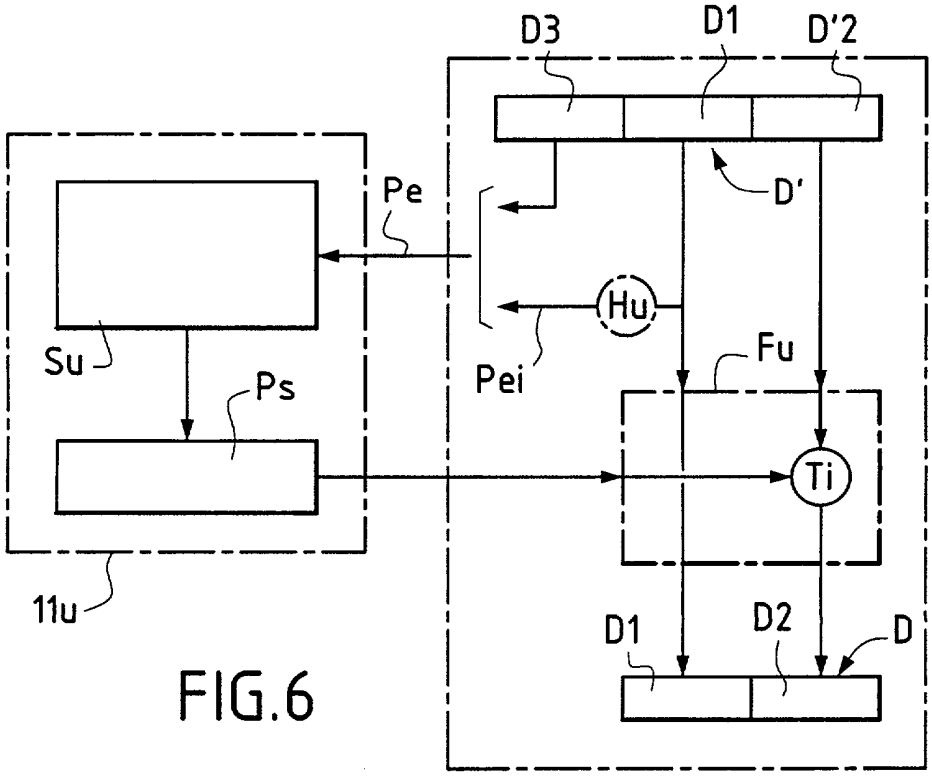

D3
D1
D'2
D'
Pe
Hu
Pei
Fu
Su
Ps
Ti
11u
D1
D2
D

FIG.6

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national
2793050

FA 578830
FR 9905570

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	EP 0 191 162 A (IBM) 20 août 1986 (1986-08-20) * colonne 2, ligne 22 - ligne 37 * * colonne 3, ligne 2 - ligne 28 * * colonne 5, ligne 9 - ligne 33 * * colonne 8, ligne 22 - colonne 9, ligne 50 * * figures 3-10 *	1-6,8,9, 13-15
Y		7,10-12
Y	EP 0 795 809 A (TOKYO SHIBAURA ELECTRIC CO) 17 septembre 1997 (1997-09-17) * abrégé; figure 2 * * colonne 14, ligne 10 - colonne 15, ligne 45 *	7
Y	"DEA-BASED PSEUDORANDOM NUMBER GENERATOR" IBM TECHNICAL DISCLOSURE BULLETIN,US,IBM CORP. NEW YORK, vol. 35, no. 1B, 1 juin 1992 (1992-06-01), pages 431-434, XP000309126 ISSN: 0018-8689 * le document en entier *	10-12
A	EP 0 768 601 A (CASIO COMPUTER CO LTD) 16 avril 1997 (1997-04-16) * abrégé; figure 1 *	4-6

DOMAINES TECHNIQUES RECHERCHES (Int.CL.7)

G06F

Date d'achèvement de la recherche	Examinateur
9 février 2000	Sigolo, A

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)