(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 747 208**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **96 04404**

(51) Int Cl[6] : **G 06 F 1/00**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 09.04.96.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 10.10.97 Bulletin 97/41.

(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) :** *CLEMOT OLIVIER* — FR, *CAMPANA MIREILLE* — FR et *ARDITTI DAVID* — FR.

(72) **Inventeur(s) :**

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

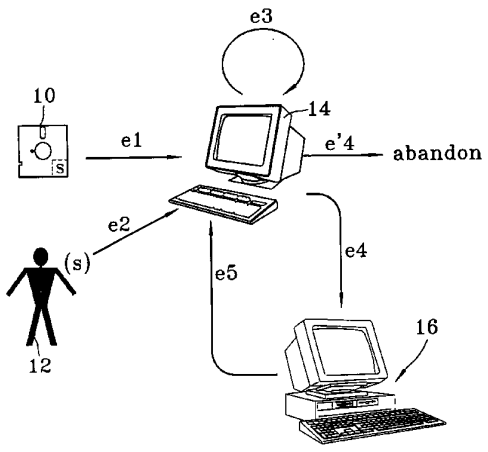
(74) **Mandataire :** SOCIETE DE PROTECTION DES INVENTIONS.

(54) PROCEDE DE DISSIMULATION D'UN CODE SECRET DANS UN DISPOSITIF D'AUTHENTIFICATION INFORMATIQUE.

(57) L'invention concerne un procédé de dissimulation d'un code secret dans un dispositif d'authentification informatique (10) consistant à crypter le code secret (s) par une fonction de cryptage (g) pour former une image de code secret (s) et à mémoriser cette image de code secret dans le dispositif d'authentification. Il consiste, au préalable, à choisir une fonction de cryptage (g) qui est telle que, à chaque image de code secret mémorisée, il correspond une pluralité de codes antécédents (s1, ..., sn) tous différents du code secret, mais qui, une fois cryptés par la fonction de cryptage (g), ont une image (s) identique à celle du code secret.

Elle concerne aussi un procédé de vérification du code secret d'un utilisateur muni d'un dispositif d'authentification dans lequel est mémorisée l'image du code secret.

Application au domaine de l'authentification informatique.



FR 2 747 208 - A1

PROCEDE DE DISSIMULATION D'UN CODE SECRET DANS UN DISPOSITIF D'AUTHENTIFICATION INFORMATIQUE

DESCRIPTION

Domaine technique

L'invention concerne un procédé pour dissimuler un code secret dans un dispositif d'authentification tel qu'une disquette informatique, une carte à mémoire,..., pouvant être lu à partir d'un lecteur adéquat.

Elle trouve des applications dans tous les systèmes informatiques mettant en oeuvre une procédure d'authentification des utilisateurs voulant se connecter, depuis un terminal, sur le système central.

Etat de la technique

Dans les systèmes informatiques actuels, la protection des données joue un rôle de plus en plus important. En effet, la qualité du système informatique dépend de manière décisive de la sécurité de l'échange de données à l'intérieur du système. On cherche donc de plus en plus à sécuriser l'accès au système, c'est-à-dire que l'on cherche à contrôler si les personnes utilisant le système sont autorisées à l'utiliser, les personnes non autorisées devant alors être refusées par le système.

Un mode de réalisation simple, mais n'offrant pas une sécurité absolue, consiste à contrôler l'accès au système informatique par la vérification du mot de passe connu uniquement de l'utilisateur autorisé et souvent changé afin de limiter la possibilité que des utilisateurs non autorisés découvrent ce mot de passe. Cependant, il y a de forts risques pour que les mots de passe soient

interceptés par des personnes non autorisées désireuses d'utiliser le système informatique.

De plus, ce mot de passe est stocké dans la zone mémoire du système informatique (zone protégée ou non) afin d'être comparé au mot de passe entré par l'utilisateur. Il peut donc être facilement retrouvé en mémoire par un utilisateur frauduleux.

Pour éviter cette fraude, une technique consiste à crypter le mot de passe avant de le stocker en mémoire. Ce cryptage se fait au moyen d'une fonction de cryptage qui est choisie, en général, de façon à ce qu'il soit impossible de retrouver le mot de passe à partir de l'image du mot de passe obtenue après cryptage de ce mot de passe. Cette technique est utilisée, par exemple, dans les systèmes UNIX®.

Dans ce cas, l'image du mot de passe est stockée en clair dans la mémoire de sorte qu'il est possible à un utilisateur frauduleux de récupérer le fichier de toutes les images de mots de passe mémorisées et ensuite d'implémenter la fonction de cryptage sur un autre système informatique et d'essayer des listes de mots de passe jusqu'à retrouver ceux qui correspondent aux images du fichier. Une telle analyse du code du système (fonction, fichier des images de mot de passe...) est appelée "attaque par dictionnaire".

Par ailleurs, il existe un procédé permettant de dissimuler un code secret en stockant, sur des moyens de stockage tels qu'une disquette, une carte à mémoire, etc., l'image du code secret par une fonction de cryptage réversible, paramétrée par le mot de passe de l'utilisateur. Ce procédé est mis en oeuvre "localement", c'est-à-dire qu'il est exécuté par le terminal, en liaison avec les moyens de stockage et qu'il ne nécessite aucune connexion vers le système central.

Ce procédé est décrit en détail dans la demande de brevet FR-A-2 690 257.

Comme expliqué dans cette demande de brevet, ce procédé permet aussi de changer le mot de passe de l'utilisateur localement, c'est-à-dire sans qu'aucune connexion au système central ne soit nécessaire. Par contre, une connexion au système est obligatoire pour vérifier la validité de ce changement de mot de passe.

L'authentification de l'utilisateur se fait donc localement : le code secret n'est jamais transmis, sur une ligne de transmission, vers le système central. L'unique transmission du code secret au cours du procédé, se fait entre le lecteur des moyens de stockage et le terminal, ce qui limite les risques d'interception par un fraudeur. La connexion sur le système central se fait ensuite, c'est-à-dire après vérification locale du code secret.

Cependant, un tel procédé nécessite une protection physique des moyens de stockage (disquette) pour éviter la fraude directement sur ces moyens de stockage. Ceci implique donc l'utilisation de matériels et de technologies spécifiques, entraînant un coût relativement important.

Exposé de l'invention

L'invention a pour but de remédier aux inconvénients des procédés décrits précédemment. A cette fin, elle propose un procédé pour dissimuler un code secret dans un dispositif d'authentification tel qu'une disquette ou une carte à mémoire. Ce procédé permet de vérifier localement le code secret entré par l'utilisateur, tout en limitant les risques d'attaques par dictionnaire.

De façon plus précise, l'invention concerne un procédé de dissimulation d'un code secret dans un dispositif d'authentification informatique consistant à

crypter le code secret par une fonction de cryptage pour former une image de code secret et à mémoriser cette image de code secret dans le dispositif d'authentification. Ce procédé se caractérise par le fait qu'il consiste, au préalable, à choisir une fonction de cryptage qui est telle que, à chaque image de code secret, il correspond une pluralité de codes antécédents tous différents du code secret, mais qui, une fois cryptés par la fonction de cryptage, ont une image identique à celle du code secret.

Avantageusement, le code secret ayant n caractères, la fonction de cryptage consiste à associer à ces n caractères une image de code secret de k caractères, avec $k < n$.

Selon un mode de réalisation préféré de l'invention, le nombre k des caractères de l'image du code secret est égal à $\frac{n}{2}$.

L'invention concerne aussi un procédé de vérification du code secret d'un utilisateur voulant accéder à un système central à partir d'un terminal. Cet utilisateur étant muni d'un dispositif d'authentification dans lequel est dissimulée l'image du code secret par la fonction de cryptage, ce procédé se caractérise par le fait qu'il comprend une étape de vérification locale du code secret entré par l'utilisateur et crypté par la fonction de cryptage, par comparaison avec l'image du code secret mémorisée dans le dispositif d'authentification ; puis, si cela est vérifié, il comporte une étape d'authentification par le système central.

Brève description des figures

- La figure 1 représente schématiquement la répartition des images du code secret dans la mémoire ainsi que des antécédents possibles de cette image ;

- les figures 2A, 2B, 3A et 3B représentent des exemples de fonctions de cryptage appliquées à un certain nombre de caractères numériques ; et

- la figure 4 représente le schéma fonctionnel du procédé de vérification du code secret.

Description détaillée de modes de réalisation de l'invention

L'invention concerne un procédé pour dissimuler un code secret dans un dispositif d'authentification tel qu'une disquette informatique ou une carte mémoire ou encore une calculette.

Ce procédé consiste à crypter le code secret par une fonction de cryptage g, de façon à former une image du code secret qui est ensuite mémorisée dans le dispositif d'authentification.

La fonction de cryptage g est choisie de façon à ce que l'image du code secret soit suffisamment précise pour qu'une faute de frappe, tapée par l'utilisateur lorsque celui-ci entre son code secret, puisse être détectée avec une probabilité tout à fait satisfaisante mais que, pourtant, chaque image du code secret possède de nombreux antécédents par la fonction de cryptage, de façon à ce qu'une attaque par dictionnaire fournisse de nombreuses fausses solutions à la vérification locale, mais pas à l'authentification distante.

En d'autres termes, la fonction de cryptage g est choisie de façon à ce que le code secret ait une image de code secret qui corresponde à une multitude de codes antécédents (appelés simplement "antécédents", dans la suite du texte). Ces codes antécédents sont une sorte de faux codes secrets, qui, codés par la fonction de cryptage g, donnent tous la même image de code secret que le

véritable code secret de l'utilisateur, mais qui seront refusés lors de la procédure d'authentification.

Ainsi, un utilisateur frauduleux qui serait en possession du dispositif d'authentification, par exemple de la disquette, et qui aurait ainsi découvert le fichier des images de codes secrets et qui, par ailleurs, serait en possession de la fonction de cryptage g, ne pourrait pas déterminer précisément quel est le code secret de l'utilisateur. En effet, une attaque par dictionnaire lui fournirait de nombreuses solutions à la vérification locale, mais une très faible chance de trouver la véritable solution, c'est-à-dire le véritable code secret. Effectivement, si l'utilisateur frauduleux essaie l'un des codes antécédents fourni par l'attaque par dictionnaire, celui-ci est vérifié localement ; par contre, il sera refusé lors de l'authentification à distance, c'est-à-dire de l'authentification par le système central.

On a représenté sur la figure 1, de façon très schématique, la répartition des images de codes secrets dans la mémoire, ainsi que la répartition des codes antécédents de ces images de codes secrets.

De façon plus précise, on a appelé "E1" l'ensemble de tous les codes qui pourraient être un code secret choisi par l'utilisateur et "E2" l'ensemble de toutes les images de ces codes secrets qui pourraient être choisis par l'utilisateur. L'ensemble E1 comporte donc tous les éventuels codes secrets, dont, en particulier, un code x et une multitude de codes s1 à sn.

Si "g" est la fonction de cryptage choisie, alors l'image du code x par la fonction de cryptage g donne l'image X qui se situe dans l'ensemble E2 des images de codes secrets possibles. D'autre part, l'image par la fonction de cryptage g de chacun des codes s1 à sn donne l'image de code secret S contenue dans l'ensemble E2.

Ce sont donc tous ces codes antécédents s1, s2, s3,..., sn qui, codés par la fonction de cryptage g, donnent une image S qui correspond aussi à l'image du véritable code secret. On comprend donc que l'un de ces codes s1 à sn est le véritable code secret choisi par l'utilisateur. Ainsi, bien que tous ces codes antécédents s1 à sn aient pour image S, l'un seulement de ces codes antécédents est le véritable code secret qui vérifiera l'authentification par le système central.

Ainsi, un utilisateur frauduleux qui serait en possession à la fois de la fonction de cryptage g et de l'image de code secret S, ne saura lequel des codes antécédents s1 à sn choisir. Aussi, s'il essaie localement, c'est-à-dire au niveau du terminal informatique, l'un de ces codes antécédents s1 à sn, la vérification par le terminal lui donnera une réponse positive, c'est-à-dire qu'une procédure d'authentification peut être mise en oeuvre. Cependant, cette procédure d'authentification n'aboutira pas et la connexion au système central sera refusée.

Par contre, la fonction de cryptage est choisie de façon à ce qu'elle fournisse des images de codes secrets suffisamment précises pour qu'une faute de frappe de la part de l'utilisateur puisse être détectée localement, c'est-à-dire sans nécessiter de connexion avec le système central.

Selon un mode de réalisation de l'invention, la fonction de cryptage g est une fonction qui associe à n caractères constituant le code secret, une image de code secret de taille réduite, c'est-à-dire de k caractères, avec $k < n$. Par exemple, pour un code secret ayant n caractères, la fonction de cryptage g associe une image de $k = n/2$ caractères. Dans le mode de réalisation préféré de l'invention, la fonction g associe à un code secret de huit

caractères (ce qui correspond à une taille d'environ 2^{40} bits), une image de code secret de quatre caractères (taille d'environ 2^{20} bits).

Pour une fonction de cryptage g de ce type, l'utilisateur qui tape le véritable code secret avec une faute de frappe aura un risque sur environ un million de cas (1 sur 2^{20}) que sa faute de frappe ne soit pas détectée lors de l'opération de vérification locale ; par contre, un utilisateur frauduleux qui tente une attaque par dictionnaire se verra confronté à environ un million de solutions (2^{20}), parmi lesquelles une seule est la bonne, c'est-à-dire qu'une seule correspond au véritable code secret.

On comprendra, bien sûr, que plusieurs fonctions peuvent être utilisées, pour vérifier les conditions énoncées précédemment. Même des fonctions très simples peuvent être utilisées. Par exemple, si l'on prend en compte les chiffres entre 0 et 9 et les lettres de l'alphabet que l'on représente par des valeurs comprises entre 10 et 35, on peut choisir une fonction g1 qui associe, à chaque couple de caractères (lettres ou chiffres) du code secret de l'utilisateur, une valeur déterminée entre 0 et 35, de telle sorte que pour un caractère donné du bigramme (c'est-à-dire du couple de caractères), l'image soit différente lorsque le deuxième caractère varie. On peut, par exemple, choisir la somme des deux valeurs du bigramme.

La figure 2A représente schématiquement le traitement effectué par la fonction g1 sur un code secret comprenant n caractères.

On a donc représenté sur cette figure 2A, les n/2 couples de caractères (c1, c2) (c3, c4)... (c1, cn) et chacune des images $Ic_1, \ldots, Ic_{n/2}$ de ces bigrammes. D'après la définition de la fonction g1, décrite précédemment,

chaque image $Ic_{n/2}$ correspond à la somme des caractères C_1 et C_n du bigramme correspondant, sachant que si la somme de ces caractères donne une valeur supérieure ou égale à 10, on choisit pour $Ic_{n/2}$ la valeur de plus faible poids, à savoir le chiffre de l'unité.

La figure 2B représente un exemple numérique du cryptage réalisé au moyen de la fonction g1. Dans cet exemple, on considère un code secret de huit caractères numériques notés c1, c2,..., c8 regroupés en quatre bigrammes dont les valeurs sont comprises entre 0 et 9 sont :

(c1, c2) = (6,1)

(c3, c4) = (5,7)

(c5, c6) = (4,3)

(c7, c8) = (9,2)

La fonction g1 associe donc à chaque bigramme, la somme des deux caractères le constituant. Ainsi :

Σ(c1, c2) = 7

Σ(c3, c4) = 2

Σ(c5, c6) = 7

Σ(c7, c8) = 1

On comprend donc, à partir de cet exemple, que l'image du code secret "61574392" est "7271". Une telle image 7271 peut avoir une multitude d'antécédents, puisque chaque caractère de cette image du code secret peut être le résultat de la somme (ou bien l'unité d'un chiffre correspondant à la somme) d'une multitude de nombres compris entre 0 et 35.

On comprend bien, de plus, que si l'utilisateur tapait le véritable code secret avec une erreur de frappe, par exemple 7 à la place de 6 pour le caractère c1, cette erreur serait tout de suite détectée localement puisque la somme de 7 et de 1 ne peut, bien évidemment, donner le

chiffre 7 qui correspond à l'image Ic1 du premier couple de caractères (c1, c2).

Sur la figure 3A, on a représenté un exemple d'une autre fonction de cryptage : la fonction g_2 qui consiste à associer à l'ensemble des huit caractères c1 à C8 composant le code secret, quatre combinaisons linéaires indépendantes, modulo 36, de ces huit caractères, chaque combinaison linéaire pouvant être différente.

Par exemple, le premier caractère Ic1 de l'image du code secret associe les caractères c1, c3, c4 et c7 du code secret ; le second caractère Ic2 de cette image du code secret associe les caractères c2, c5, c6 et c8 ; le troisième caractère de l'image du code secret Ic3 associe les caractères c1, c2, c5 et c7, et le quatrième caractère Ic4 de l'image du code secret associe les caractères c3, c4, c5 et c7 du code secret initial.

Sur la figure 3B, on a représenté le même exemple que celui de la figure 3A, mais dans lequel on a attribué à chaque caractère une valeur numérique qui est la même que celle donnée dans l'exemple de la figure 2B. Ainsi :

c1 = 6
c2 = 1
c3 = 5
c4 = 7
c5 = 4
c6 = 3
c7 = 9
c8 = 2

Après cryptage, par la fonction g2, d'un code secret de huit caractères c1 à c8, où c1,..., c8 ont les valeurs ci-dessus, on obtiendra une image de code secret 7007, avec Ic1 = 7, Ic2 = 0, Ic3 = 0, Ic4 = 7.

Ainsi, le procédé de dissimulation du code secret sur le dispositif d'authentification présente donc l'avantage, non seulement de détecter une éventuelle faute de frappe de la part de l'utilisateur lorsque celui-ci entre son code secret sur le terminal, mais surtout d'éviter une attaque par dictionnaire de la part d'un utilisateur frauduleux, puisque l'image du code secret mémorisée sur la disquette à un tel nombre de codes antécédents possibles qu'un utilisateur frauduleux a très peu de chance de trouver le véritable code secret.

Le procédé décrit ci-dessus pour dissimuler un code secret dans une disquette informatique, une carte à mémoire, ou tout autre dispositif d'authentification, peut être utilisé dans un procédé de vérification du code secret entré par un utilisateur désirant accéder à un système central, à partir d'un terminal connecté à un lecteur apte à lire son dispositif d'authentification.

Pour une meilleure compréhension de l'invention, le procédé de vérification du code secret va être décrit dans le cas où le dispositif d'authentification est une disquette informatique.

Ce procédé de vérification consiste, après que la disquette ait été introduite dans le lecteur de disquettes associé au terminal, à ce que l'utilisateur entre son code secret sur le terminal à partir duquel il désire se connecter au système central. Le terminal vérifie alors si l'image, par la fonction de cryptage g, du code secret s que vient de taper l'utilisateur correspond à l'image S mémorisée sur la disquette. Si cela n'est pas le cas, alors le terminal refuse toute connexion vers le système central. Au contraire, si cela est vérifié, alors une étape de détermination de la clé secrète non chiffrée K est commencée, au terme de laquelle le terminal se connectera au système central. Cette clé secrète non

chiffrée K est déterminée à partir de l'inverse f^{-1} de la fonction de chiffrage f de la clé par le mot de passe (f étant une fonction réversible), et à partir de la clé chiffrée stockée sur la disquette, tel que cela est expliqué dans la demande de brevet FR-A-2 690 257, déjà citée précédemment.

La procédure d'authentification qui est mise en oeuvre dès que le terminal informatique se connecte sur le système central, ne sera donc pas décrite ici puisqu'elle est identique à celle décrite dans le document FR-A-2 690 257.

Un diagramme fonctionnel de ce procédé de vérification du code secret est représenté sur la figure 4.

La disquette informatique, référencée 10, est introduite dans le terminal informatique 14 lors d'une étape e1. L'utilisateur, référencé 12, entre ensuite son code secret (s) sur le terminal 14 lors d'une étape e2. Une étape e3 est alors effectuée qui consiste à crypter par la fonction g, le code secret s que l'utilisateur vient d'entrer puis à vérifier si l'image du code secret par la fonction g correspond bien à l'image de code secret s mémorisée sur la disquette 10. Si ce n'est pas le cas, alors le procédé de vérification est abandonné (étape e'4) et donc aucune procédure d'authentification par le système central n'est envisagée. Au contraire, si cette vérification s'avère exacte, une étape e4 est effectuée. Cette étape e4 consiste à déterminer la clé secrète non chiffrée K et à l'envoyer au système central 16 qui commence alors la procédure d'authentification (étape e5), au moyen d'un échange d'informations avec le terminal 14.

Ainsi, le procédé de vérification du code secret assure une limitation du nombre de connexions au système central, puisque seuls les codes secrets acceptés lors de la vérification locale du code secret font l'objet d'une procédure d'authentification.

De plus, l'image du code secret étant mémorisée sur le dispositif d'authentification, et non dans une mémoire accessible à tous un utilisateur frauduleux désirant connaître cette image de code secret doit tout d'abord s'emparer de ce dispositif d'authentification, ce qui participe à la limitation des fraudes.

REVENDICATIONS

1. Procédé de dissimulation d'un code secret dans un dispositif d'authentification informatique (10) consistant à crypter le code secret (s) par une fonction de cryptage (g) pour former une image de code secret (s) et à mémoriser cette image de code secret dans le dispositif d'authentification, caractérisé en ce qu'il consiste, au préalable, à choisir une fonction de cryptage (g) qui est telle que, à chaque image de code secret mémorisée, il correspond une pluralité de codes antécédents (s1,..., sn) tous différents du code secret, mais qui, une fois cryptés par la fonction de cryptage (g), ont une image (s) identique à celle du code secret.

2. Procédé de dissimulation d'un code secret selon la revendication 1, caractérisé en ce que le code secret ayant n caractères (c1,..., cn), la fonction de cryptage (g) consiste à associer à ces n caractères (c1,..., cn) une image de code secret de k caractères, avec $k < n$.

3. Procédé de dissimulation d'un code secret selon la revendication 2, caractérisé en ce que le nombre k des caractères de l'image du code secret est égal à $\frac{n}{2}$.

4. Procédé de vérification du code secret d'un utilisateur voulant accéder à un système central à partir d'un terminal, caractérisé en ce que, cet utilisateur (12) étant muni d'un dispositif d'authentification (10) dans lequel est mémorisée l'image (s) du code secret par la fonction de cryptage (g) conformément à l'une quelconque des revendications 1 à 3, il comprend une étape (e3) de vérification locale du code secret entré par l'utilisateur et crypté par la fonction de cryptage, par comparaison avec l'image du code secret mémorisée dans le dispositif d'authentification, puis si cela est vérifié, une étape (e5) d'authentification par le système central (16).

FIG. 1

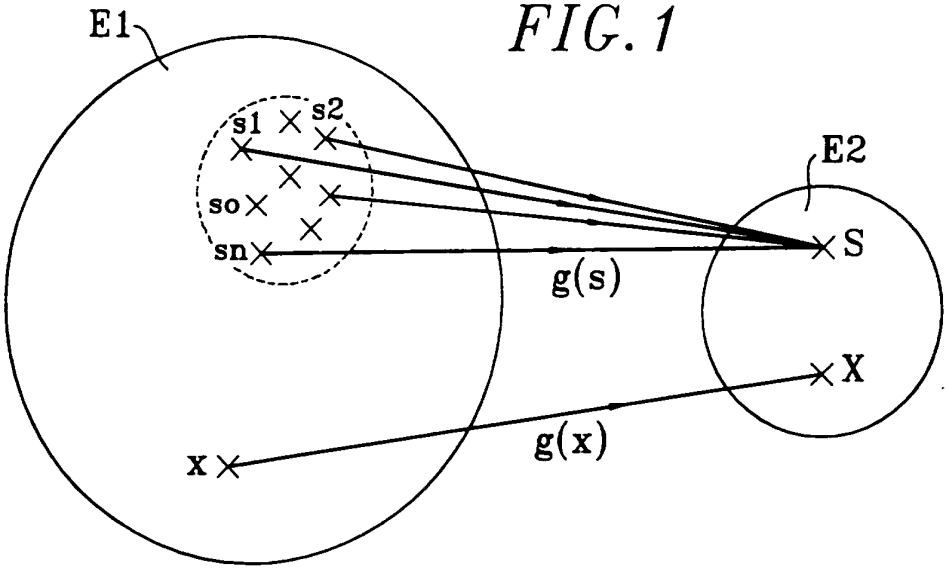
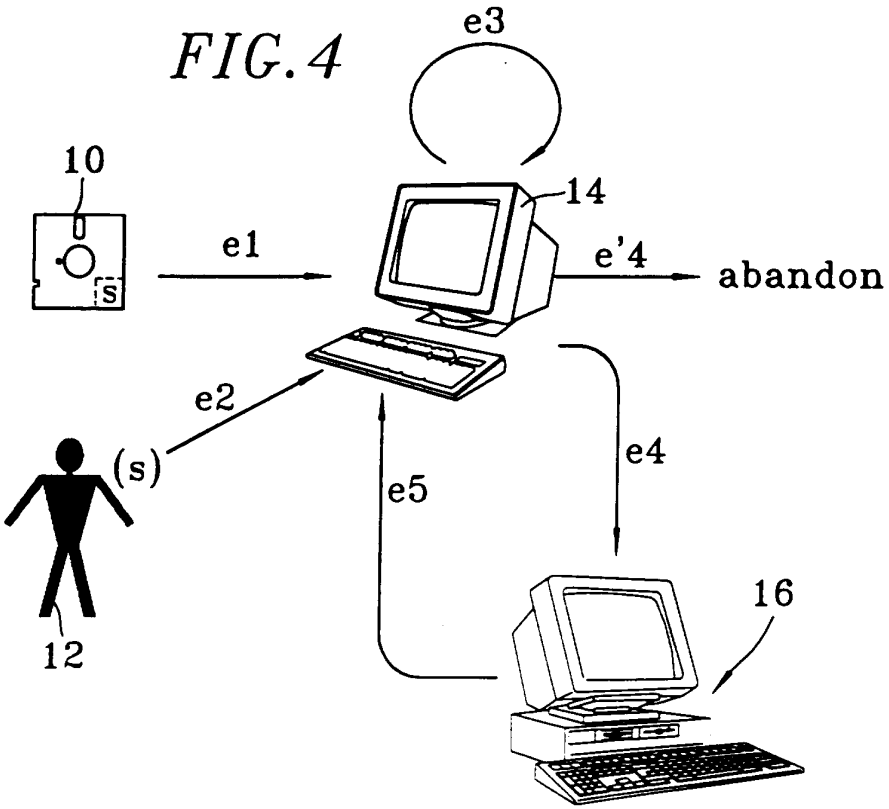


FIG. 4



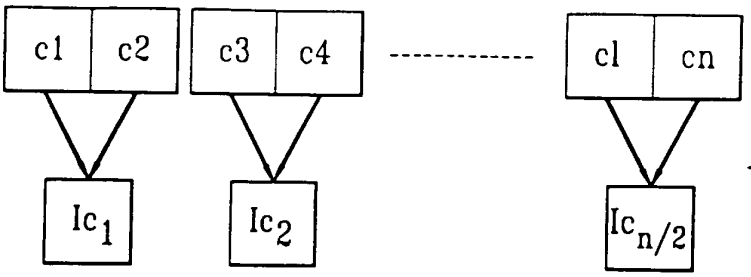


FIG.2A

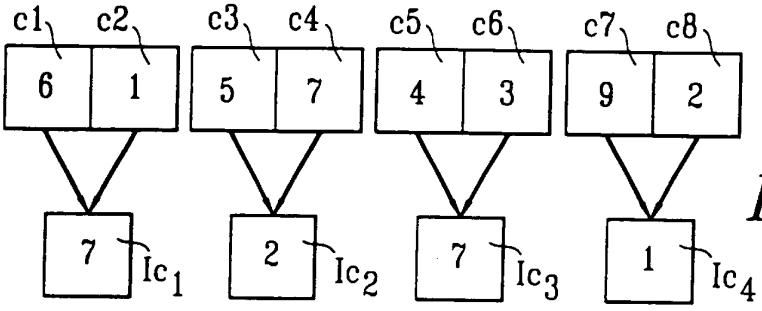


FIG.2B

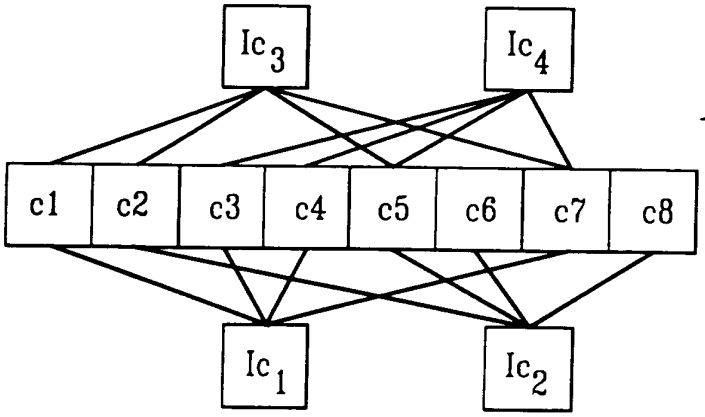


FIG.3A

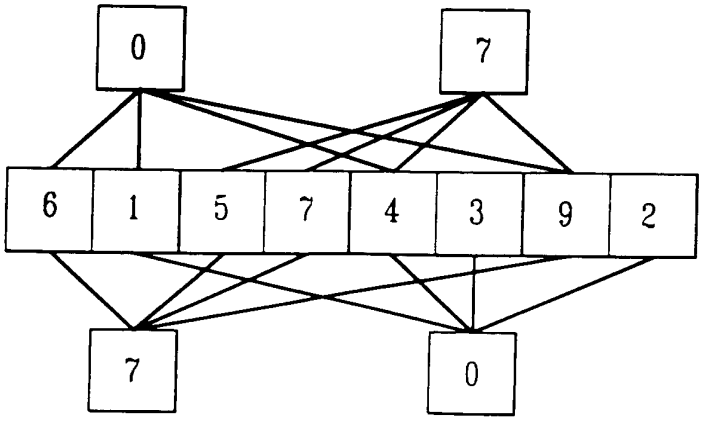


FIG.3B

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

2747208
N° d'enregistrement national

FA 530538
FR 9604404

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
Y	EP-A-0 191 324 (IBM) 20 Août 1986 * abrégé; figures 1,2 * * colonne 2, ligne 42 - colonne 3, ligne 7 * * revendication 1 *	1-3
A		4

Y	COMPUTERS & SECURITY INTERNATIONAL JOURNAL DEVOTED TO THE STUDY OF TECHNICAL AND FINANCIAL ASPECTS OF COMPUTER SECURITY, vol. 11, no. 5, 1 Septembre 1992, pages 427-437, XP000296996 BAUSPIESS F ET AL: "REQUIREMENTS FOR CRYPTOGRAPHIC HASH FUNCTIONS" * le document en entier *	1-3
A		4

A	PHILIPS TELECOMMUNICATION REVIEW, vol. 47, no. 3, 1 Septembre 1989, pages 1-19, XP000072642 FERREIRA R C: "THE SMART CARD: A HIGH SECURITY TOOL IN EDP" * figures 4,6 * * page 5, ligne 6 - page 7, ligne 5 * * page 9, ligne 1 - page 11, ligne 4 *	1,4

A	US-A-5 233 655 (SHAPIRO SANFORD S) 3 Août 1993 * abrégé *	2,3

D,A	FR-A-2 690 257 (FRANCE TELECOM ;ALLEGRE FRANCOIS; ARDITTI DAVID; CAMPANA MIREILLE) 22 Octobre 1993 * le document en entier *	1,4

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.6)

G06F
H04L

Date d'achèvement de la recherche	Examinateur
19 Décembre 1996	Powell, D

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)