(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 773 406**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **98 00051**

(51) Int Cl^6 : **G 07 F 7/10,** H 04 L 9/32 // G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 06.01.98.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 09.07.99 Bulletin 99/27.

(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) :** *SCHLUMBERGER INDUSTRIES SA Societe anonyme* — FR.

(72) **Inventeur(s) :** SALLE PATRICK.

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

(74) **Mandataire(s) :** PATCO SA.

(54) PROCEDE D'AUTHENTIFICATION DE CARTES A CIRCUIT INTEGRE.

(57) Procédé d'authentification de cartes à circuit intégré par un organe vérificateur, le procédé mettant en oeuvre un algorithme comprenant les étapes de:

- calculer un module N en faisant le produit de deux nombres premiers P et Q secrets,
- déterminer de façon aléatoire k valeurs d'authentification V_1,
- implanter dans une mémoire de chaque carte k clés secrètes S_1 tel que $S_1 = V_1^{-1/2}$ (mod N),
- déterminer aléatoirement dans la carte un nombre R et calculer $X = R^2$ (mod N), et transmettre X à l'organe vérificateur,
- déterminer aléatoirement dans l'organe vérificateur un nombre-test E composé de k bits e_1 transmis à la carte,
- calculer dans la carte $Y = R \prod S_1^{e1}$ (mod N) pour i variant de 1 à k,
- contrôler dans l'organe vérificateur que $x = Y^2 \prod V_1^{e1}$ (mod N) pour i variant de 1 à k,

les valeurs d'authentification V_1 étant communes à toutes les cartes et chaque carte contenant un module N_3 qui lui est propre, le procédé comprenant l'étape de transmettre le module N_j à l'organe vérificateur préalablement au calcul de contrôle de X par l'organe vérificateur.

FR 2 773 406 - A1

La présente invention concerne un procédé d'authentification de cartes à circuit intégré, telles que des cartes bancaires ou d'autorisation d'accès, par un organe vérificateur tel qu'un terminal informatique.

On sait qu'un algorithme RSA (abréviation des noms de ses auteurs, RIVERST, SHAMIR, ADELMAN) est utilisé actuellement pour l'authentification de cartes à circuit intégré. Pour la mise en oeuvre de cet algorithme on utilise un exposant public E. Pour chaque carte, un module N est calculé en effectuant le produit de deux nombres premiers P et Q secrets et un exposant secret D est calculé de façon que $D \times E = 1 \bmod (P-1)(Q-1)$. Ces valeurs sont ensuite mémorisées dans la carte concernée. Lorsque la carte à circuit intégré est connectée à l'organe vérificateur, le module N et l'exposant public E sont transmis par la carte à l'organe vérificateur tandis que les facteurs premiers P et Q ainsi que l'exposant D demeurent secrets. Pour authentifier la carte, l'organe vérificateur sélectionne aléatoirement une valeur-test R et la transmet à la carte. La carte calcule une preuve $Pr = R^D \pmod N$ et la transmet à l'organe vérificateur. L'organe vérificateur contrôle alors que $R = Pr^E \pmod N$. Afin d'obtenir une sécurité suffisante avec cet algorithme, il est nécessaire d'utiliser un module N et un exposant secret D de grande dimension. La carte doit donc disposer d'un espace-mémoire important pour mémoriser ces valeurs. De plus, la carte doit effectuer de nombreux calculs de sorte que la carte emploie des moyens de calcul importants.

On connaît par ailleurs du document US-A-4,748,668 un algorithme dit de Fiat Shamir comprenant les étapes de :

- calculer un module N en faisant le produit de deux nombres premiers P et Q secrets,
- déterminer de façon aléatoire k valeurs d'authentification V_i,

- implanter dans une mémoire de chaque carte k clés secrètes S_i tel que $S_i = V_i^{-1/2} \pmod N$,

- déterminer aléatoirement dans la carte un nombre R et calculer $X = R^2 \pmod N$, et transmettre X à l'organe vérificateur,

- déterminer aléatoirement dans l'organe vérificateur un nombre-test E composé de k bits e_i transmis à la carte,

- calculer dans la carte $Y = R \Pi S_i^{e_i} \pmod N$ où Π désigne l'opération de produit modulaire des k facteurs $S_i^{e_i}$ pour i variant de 1 à k,

- contrôler dans l'organe vérificateur que $X = Y^2 \Pi V_i^{e_i} \pmod N$ pour i variant de 1 à k.

Dans cet algorithme, les valeurs d'authentification varient d'une carte à une autre. Pour effectuer la vérification, l'organe vérificateur doit connaître les valeurs d'authentification propres à la carte. Les valeurs d'authentification peuvent être soit mémorisées dans l'organe vérificateur, ce qui est irréaliste si le nombre de cartes est important ; soit être transmises à l'organe vérificateur par chaque carte, ce qui suppose de stocker ces valeurs dans la carte avec la signature permettant de les valider. Ceci impose une charge de stockage pour la carte, augmente le nombre de messages à transmettre et la charge de travail pour l'organe vérificateur.

En outre, dans cet algorithme, le module N est commun à toutes les cartes de sorte que si un fraudeur parvient à factoriser le nombre N en ses facteurs P et Q, le fraudeur pourra déterminer les clés secrètes S_i de toutes les cartes du réseau à partir des valeurs d'authentification V_i qui sont accessibles. Le fraudeur pourra alors introduire ces clés dans des fausses cartes et utiliser celles-ci comme si elles bénéficiaient d'une identification authentique. Afin d'obtenir un degré de sécurité important, il est donc nécessaire de choisir un nombre N de grande

dimension augmentant ainsi la difficulté de sa factorisation. Toutefois, ceci augmente la charge de calcul de la carte et l'espace-mémoire nécessaire.

Selon l'invention, on propose un procédé d'authentification de cartes à circuit intégré par un organe vérificateur, mettant en oeuvre un algorithme analogue à l'algorithme de Fiat Shamir et dans lequel les valeurs d'authentification V_i sont communes à toutes les cartes et chaque carte contient un module N_j qui lui est propre, le procédé comprenant l'étape de transmettre le module N_j à l'organe vérificateur préalablement au calcul de contrôle de X par l'organe vérificateur.

Le module N_j étant propre à chaque carte, un fraudeur parvenant à factoriser le module N_j ne pourra utiliser que ce module et non pas forcer tout le système d'authentification. Pour déjouer la fraude, il suffira donc de mettre ce module hors service, les autres cartes du réseau pouvant être utilisées normalement. En conséquence, le module N_j ne servant à la protection que d'une carte, il peut être de dimension réduite. Le procédé d'authentification est de la sorte applicable à des cartes disposant d'un espace-mémoire et de moyens de calcul limités.

Avantageusement, le module N_j est mémorisé dans la carte sous forme de ses facteurs premiers P_j et Q_j.

La carte disposant des deux facteurs premiers, les calculs sont simplifiés. L'espace-mémoire utilisé par la carte pour l'exécution des calculs peut alors être minimisé.

Un mode de réalisation particulier non limitatif de l'invention va maintenant être décrit.

Le procédé d'authentification selon l'invention comprend les étapes de déterminer de façon aléatoire k valeurs d'authentification V_i publiques, et de mémoriser ces valeurs d'authentification V_i dans une mémoire de l'organe vérificateur. Le nombre k est par exemple compris entre 10

et 20, l'authentification étant d'autant plus sûre que k est élevé mais le temps de calcul étant augmenté de façon correspondante.

L'organisme chargé de l'implantation des données dans la mémoire du circuit intégré des cartes détermine aléatoirement, pour chaque carte, deux facteurs premiers P_j et Q_j. Pour certaines applications particulières, des contraintes pourront être instaurées pour la sélection des facteurs P_j et Q_j. L'ordre de grandeur des facteurs P_j et Q_j pourra notamment être déterminé en fonction du nombre de cartes mises en service, les facteurs premiers P_j et Q_j ont par exemple un ordre de grandeur de 2^{300} pour un million de cartes mises en service.

Le produit des facteurs premiers P_j et Q_j est égal au module N_j propre à chaque carte. Le module N_j est mémorisé dans la carte sous forme des facteurs P_j et Q_j .

L'organisme d'implantation calcule ensuite k clés secrètes S_i tels que $S_i = V_i^{-1/2} \pmod{N_j}$ et les mémorise dans la carte.

Une signature T_j contenant l'identification et le module N_j de la carte est mémorisée dans chaque carte.

Lorsqu'une carte est utilisée, elle est connectée à l'organe vérificateur et transmet sa signature T_j à l'organe vérificateur. L'organe vérificateur contrôle la signature T_j et en extrait le module N_j.

Le protocole d'authentification débute alors. La carte détermine aléatoirement un nombre R et effectue le calcul de $X = R^2 \pmod{N_j}$. La carte transmet le nombre X à l'organe vérificateur.

L'organe vérificateur détermine ensuite de façon aléatoire un nombre-test E composé de k bits e_i et transmet les k bits e_i à la carte.

La carte calcule alors $Y = R \prod S_i^{ei} \pmod{N_j}$ pour i variant de 1 à k et transmet le résultat Y à l'organe vérificateur.

Ensuite, l'organe vérificateur contrôle que $X = Y^2 \Pi V_i^{ei} \pmod{N_j}$ pour i variant de 1 à k. Si X = Y, il est prouvé que la carte est bien en possession des k clés secrètes S_i. La carte est alors acceptée. Avant d'accepter la carte, on peut prévoir de renouveler le protocole d'authentification un certain nombre de fois afin d'augmenter la sûreté de l'authentification.

Bien entendu l'invention n'est pas limitée au mode de réalisation décrit et on peut y apporter des variantes de réalisation sans sortir du cadre de l'invention tel que défini par les revendications.

REVENDICATIONS

1. Procédé d'authentification de cartes à circuit intégré par un organe vérificateur, le procédé mettant en oeuvre un algorithme comprenant les étapes de :

- calculer un module N en faisant le produit de deux nombres premiers P et Q secrets,

- déterminer de façon aléatoire k valeurs d'authentification V_i,

- implanter dans une mémoire de chaque carte k clés secrètes S_i tel que $S_i = V_i^{-1/2} \pmod N$,

- déterminer aléatoirement dans la carte un nombre R et calculer $X = R^2 \pmod N$, et transmettre X à l'organe vérificateur,

- déterminer aléatoirement dans l'organe vérificateur un nombre-test E composé de k bits e_i transmis à la carte,

- calculer dans la carte $Y = R \Pi S_i^{e_i} \pmod N$ pour i variant de 1 à k,

- contrôler dans l'organe vérificateur que $X = Y^2 \Pi V_i^{e_i} \pmod N$ pour i variant de 1 à k,

caractérisé en ce que les valeurs d'authentification V_i sont communes à toutes les cartes et en ce que chaque carte contient un module N_j qui lui est propre, le procédé comprenant l'étape de transmettre le module N_j à l'organe vérificateur préalablement au calcul de contrôle de X par l'organe vérificateur.

2. Procédé d'authentification selon la revendication 1, caractérisé en ce que le module N_j est mémorisé dans la carte sous forme de ses facteurs premiers P_j et Q_j.

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

FA 554364
FR 9800051

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y,D	EP 0 252 499 A (YEDA RESEARCH AND DEVELOPMENT COMPANY) 13 janvier 1988 * abrégé; revendications; figures * * page 3, ligne 43 - ligne 45 *	1
Y	EP 0 325 238 A (YEDA RESEARCH AND DEVELOPMENT COMPANY) 26 juillet 1989 * le document en entier *	1
A	WO 89 11706 A (NCR CORPORATION) 30 novembre 1989 * abrégé; revendications * * page 14, ligne 28 - ligne 36 * * page 19, ligne 4 - ligne 11 *	1
A	GB 2 154 344 A (NATIONAL RESEARCH DEVELOPMENT CORPORATION) 4 septembre 1985 * abrégé; revendications; figures *	1
A	EP 0 723 251 A (TANDEM COMPUTERS) 24 juillet 1996	
A	EP 0 496 459 A (THOMSON CONSUMER ELECTRONICS) 29 juillet 1992	
A	EP 0 311 470 A (ÉTAT FRANCAIS) 12 avril 1989	

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F
H04L

Date d'achèvement de la recherche	Examinateur
28 octobre 1998	David, J

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)