(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 807 245**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 04313**

(51) Int Cl[7] : **H 04 L 9/28,** G 06 K 19/073, G 07 F 7/12

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 30.03.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 05.10.01 Bulletin 01/40.

(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) :** *FRANCE TELECOM Société anonyme* — FR.

(72) **Inventeur(s) :** GIRAULT MARC et GILBERT HENRI.

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

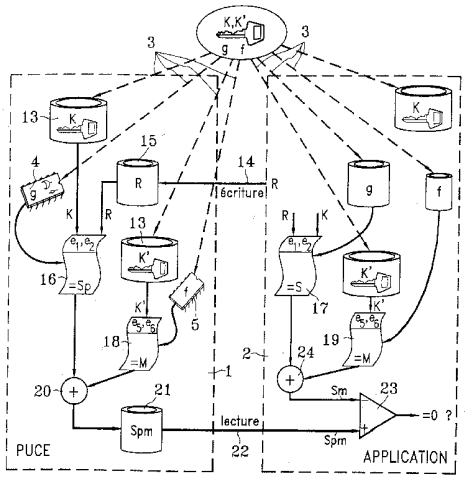
(74) **Mandataire(s) :** FRANCE TELECOM.

(54) PROCEDE DE PROTECTION D'UNE PUCE ELECTRONIQUE CONTRE LA FRAUDE.

(57) La présente invention se rapporte à un procédé de protection d'une puce électronique (1) d'un utilisateur contre la fraude dans des transactions entre une application (2) et la puce électronique (2).

Le procédé consiste:

- à calculer (16, 17) un certificat (Sp, S), par la puce électronique (1) et l'application (2), le certificat (Sp, S) étant le résultat de la fonction logique g appliquée à une liste d'arguments (e_1 , e_2) comprenant au moins l'aléa R et la clé secrète K,
- à attribuer à la puce électronique (1) une seconde clé secrète K' connue seulement de la puce électronique (1) et de l'application (2), et gardée secrète (13) dans la puce électronique (1),
- à chaque authentification de la puce électronique (1) à déterminer (18, 19) un masque M calculé en appliquant une fonction non linéaire f à au moins une partie de la clé secrète K',
- à masquer (20) la valeur du certificat (Sp) au moyen du masque M pour rendre disponible à l'application (2) uniquement la valeur du certificat masquée (Spm),
- à vérifier par l'application (2) la valeur masquée (Spm) du certificat calculée par la puce électronique (1).



FR 2 807 245 - A1

2807245

La présente invention se rapporte à un procédé de protection d'une puce électronique d'un utilisateur contre la fraude.

L'invention trouve une application très avantageuse en ce qu'elle permet de protéger contre la fraude des puces à circuit intégré à logique câblée ou à microprocesseur, notamment les puces électroniques qui équipent les cartes prépayées utilisées dans des transactions diverses telles que l'établissement de communications téléphoniques, le paiement d'objets dans un distributeur automatique, la location d'emplacements de stationnement à partir d'un parcmètre, le paiement d'un service comme un transport public ou comme la mise à disposition d'infrastructures (péage, musée, bibliothèque, ...).

Actuellement, les cartes prépayées sont susceptibles de subir différents types de fraudes. Un premier type de fraude consiste à dupliquer sans autorisation la carte, le terme clonage étant souvent utilisé pour caractériser cette opération. Un deuxième type de fraude consiste à modifier les données attachées à une carte, en particulier le montant du crédit inscrit dans la carte. Pour lutter contre ces fraudes il est fait appel à la cryptographie, d'une part pour assurer l'authentification de la carte au moyen d'une authentification et/ou pour assurer l'authentification des données au moyen d'une signature numérique et, d'autre part pour assurer la confidentialité des données au moyen d'un chiffrement. La cryptographie met en jeu deux entités, un vérificateur et un objet à vérifier, et elle peut être soit symétrique, soit asymétrique. Lorsqu'elle est symétrique, les deux entités partagent exactement la même information, en particulier une clé secrète, lorsqu'elle est asymétrique une des deux entités possède une paire de clés dont l'une est secrète et l'autre est publique ; il n'y a pas de clé secrète partagée. Dans de nombreux systèmes, seule la cryptographie symétrique est mise en œuvre avec des cartes prépayées car la cryptographie asymétrique reste lente et coûteuse. Les premiers mécanismes d'authentification développés en cryptographie symétrique consistent à calculer une fois pour toutes un certificat, différent pour chaque carte, à le stocker dans la mémoire de la carte, à le lire à chaque transaction et à le vérifier en interrogeant une application du réseau supportant la transaction où sont stockés les certificats déjà attribués. Ces mécanismes assurent une protection insuffisante. En effet, le certificat peut être espionné, reproduit et rejoué frauduleusement car il est toujours le même pour une carte donnée. Pour tenir compte du nombre faible d'authentification mis en jeu entre deux rechargements dans le cas d'une carte

prépayée rechargeable ou, au cours de la durée de vie d'une carte prépayée non rechargeable, les mécanismes d'authentification passifs sont remplacés ou complétés par des mécanismes qui font intervenir une clé secrète à des fins d'authentification ou d'acquittement d'une instruction et/ou à des fins d'authentification de données. La clé secrète, différente pour chaque carte et inscrite initialement dans la carte ou, dans le cas d'une carte rechargeable, réinscrite dans la carte lors d'un rechargement, est utilisée par la carte elle-même pour calculer un certificat lors de chaque authentification.

Un premier de ces mécanismes fait l'objet du brevet FR 89 09734. Le procédé décrit consiste à déterminer une fonction non linéaire, cette fonction étant connue de l'application et implantée dans une puce électronique sous la forme d'un automate d'états. Lors d'une authentification, la puce électronique et l'application calculent un certificat qui est le résultat de la fonction appliquée à une liste d'arguments déterminée à chaque authentification ; la liste d'arguments pouvant comprendre un aléa, l'aléa étant une donnée déterminée par l'application à chaque authentification, une donnée contenue dans la puce électronique et une clé secrète connue de la puce électronique et de l'application. Lorsque le certificat calculé par la puce électronique est identique au certificat calculé par l'application, la puce électronique est jugée authentique et la transaction entre la puce électronique et l'application est autorisée.

Un second mécanisme de protection des cartes par authentification active, faisant appel à une fonction logique basée sur l'utilisation d'un code d'authentification assurant une sécurité inconditionnelle pour un nombre limité d'authentifications, fait l'objet du brevet FR 95 12144 et est également décrite dans l'article « Solutions for Low Cost Authentication and Message Authentication » paru dans les actes de la conférence CARDIS'98. L'utilisation d'une telle fonction logique assure une protection contre le rejeu et une usure contrôlée de la clé secrète. Dans les applications basées sur la carte à mémoire considérées dans le présent brevet, on peut avantageusement faire appel à une fonction logique linéaire dépendant d'une clé secrète et de paramètres comme l'aléa reçu par la carte et le cas échéant des données internes à la carte ou reçues par la carte. La famille de fonctions logiques décrite dans le brevet FR 95 12144 constitue un cas particulier particulièrement adapté aux contraintes des cartes synchrones et faisant appel à des calculs de produits scalaires modulo 2 entre vecteurs binaires.

Chacun des deux mécanismes précédemment cités possède des avantages et des inconvénients spécifiques. En ce qui concerne le premier mécanisme, qui repose sur l'hypothèse (non prouvable dans l'état actuel des connaissances) de la sécurité

informatique de la fonction non linéaire utilisée, les très fortes contraintes imposées par les capacités de calculs réduites des puces à logique câblée n'autorisent pas une marge de sécurité aussi large que pour les algorithmes à clé secrète usuels et de ce fait la divulgation de la spécification détaillée de la fonction non linéaire utilisée peut représenter un risque. En ce qui concerne le second mécanisme, il possède l'avantage de bénéficier d'une sécurité prouvable tant que le nombre d'authentifications n'excède pas un certain seuil, et il n'y a donc pas de risque lié à la divulgation de la fonction linéaire utilisée mais, par contre la nécessité de limiter strictement le nombre d'utilisations de la fonction d'authentification pour la durée de vie de la puce (ou dans le cas de cartes rechargeables, entre deux rechargements) inhérente à cette solution peut représenter une contrainte difficile à satisfaire pour certaines applications. En outre, des attaques portant non pas sur les puces à logique câblée mais, sur les modules de sécurité utilisés pour la vérification de ces puces et, selon lesquelles un fraudeur fournirait à des modules de vérification des réponses aléatoires jusqu'à ce qu'un nombre suffisant de bonnes réponses, obtenues par hasard, lui fournisse le secret associé à un numéro de carte de son choix, peuvent être plus difficiles à contrer dans le cas du second mécanisme.

Aussi, le problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de protection d'une puce électronique d'un utilisateur contre la fraude qui comprend les étapes consistant :

- à déterminer une fonction logique g connue de l'application et implantée dans la puce électronique,
- à attribuer à la puce électronique une première clé secrète K, connue seulement de la puce électronique et de l'application, et gardée secrète dans la puce électronique,
- à chaque authentification de la puce électronique à générer un mot d'entrée variable R appelé aléa,
- à calculer un certificat, par la puce électronique et l'application, le certificat étant le résultat de la fonction logique g appliquée à une liste d'arguments comprenant au moins l'aléa R et la clé secrète K et,

qui assure une sécurité accrue.

Une solution au problème technique posé consiste, selon la présente invention, en ce que ledit procédé comprend en outre les étapes consistant :

- à déterminer une fonction non linéaire f connue de l'application et implantée dans la puce électronique,

- à attribuer à la puce électronique une seconde clé secrète K' connue seulement de la puce électronique et de l'application, et gardée secrète dans la puce électronique,
- à chaque authentification de la puce électronique à déterminer un masque M au moyen de la fonction non linéaire f appliquée à une liste d'arguments contenant au moins une partie de la clé secrète K',
- à masquer la valeur du certificat au moyen du masque M pour rendre disponible à l'application uniquement la valeur du certificat masquée,
- à vérifier par l'application la valeur masquée du certificat calculée par la puce électronique.

Ainsi, le procédé selon l'invention, qui concerne la protection d'une puce électronique contre la fraude dans des transactions entre la puce électronique et une application, masque la valeur du certificat S calculée par la puce électronique, avant que l'application le lise pour en vérifier sa valeur et déterminer si la puce électronique est authentique ; le calcul du certificat S et la détermination du masque M faisant intervenir respectivement, une fonction logique dépendante d'une première clé implantée dans la puce électronique et une fonction non linéaire dépendante d'une seconde clé également implantée dans la puce électronique, les fonctions et les clés étant connues de l'application.

Le procédé conforme à l'invention résout le problème posé car la valeur du certificat S, calculé par la puce électronique, n'est pas disponible en clair mais sous une forme masquée. Par conséquent, le fraudeur ne peut pas simplement intercepter le résultat de calcul échangé entre la puce électronique et l'application et le rejouer ultérieurement. Il lui faut connaître la valeur de la fonction logique et de la première clé qui permettent de calculer le certificat et, la valeur de la fonction non linéaire et de la seconde clé qui interviennent pour déterminer le masque.

L'application vérifie l'exactitude de la valeur masquée soit, après avoir calculé les valeurs du certificat et du masque M, à masquer au moyen du masque M la valeur du certificat et à comparer cette valeur masquée à celle calculée par la puce électronique soit, en démasquant le certificat masqué calculé par la puce électronique au moyen de la fonction inverse du masque et en comparant la valeur démasquée à la valeur du certificat calculé par l'application. Lorsque les valeurs comparées sont identiques, la puce électronique est jugée authentique et la transaction entre la puce électronique et l'application est autorisée.

De manière avantageuse, un mode particulier de mise en œuvre permet d'assurer simultanément l'authentification de la carte et l'authentification de données en faisant intervenir la valeur de certaines données dans le calcul du certificat. Dans un premier cas, ces données peuvent être mémorisées dans la puce électronique et être constituées par le numéro de la puce électronique ou par un crédit associé à la puce électronique. Dans un second cas, ces données sont écrites dans la puce électronique par l'application lors de l'opération d'authentification.

Bien qu'il soit préférable d'utiliser des clés K et K' indépendantes, il peut exister un lien de dépendance sous la forme d'une fonction qui permet de calculer la clé K' à partir de la clé K. L'attribution des clés à une puce électronique est effectuée, soit lors de la personnalisation de la puce en fin de fabrication, soit lors d'une opération de rechargement de la puce électronique dans le cas d'une puce électronique rechargeable.

Selon un autre mode particulier de mise en œuvre, la détermination des clés K et K' peut être effectuée par l'application d'une méthode de diversification ayant pour arguments d'entrée le numéro de la puce électronique et un code secret maître, ce qui permet avantageusement à l'application de reconstituer les clés secrètes de chaque puce électronique après lecture du numéro de la puce ; aucun stockage des clés secrètes des puces n'est alors nécessaire.

Selon un autre mode particulier de mise en œuvre, la clé K est un mot d'un nombre déterminé de bits regroupés en séquences K[i], chaque séquence K[i] ayant un nombre de bits égal au nombre de bits des arguments d'entrée autre que la clé K et pris comme un tout et, la fonction logique g consiste à effectuer des produits scalaires modulo 2 entre chacun des bits d'une séquence déterminée K[i] et les bits des arguments d'entrée autre que la clé K.

La fonction non linéaire f peut avoir comme arguments d'entrée soit la clé K', soit l'aléa R, soit des données D internes à la puce électronique, soit des données D' fournies à la puce électronique par l'application, soit une combinaison de ces derniers ; chaque argument ajoutant une difficulté à surmonter pour le fraudeur.

Selon un autre mode particulier de mise en œuvre, l'aléa R est déterminé par l'application à partir d'un nombre aléatoire généré par l'application et l'aléa R est transmis à la puce électronique par l'application.

Selon un autre mode particulier de mise en œuvre, l'aléa R est déterminé à partir d'une suite d'entiers consécutifs générés par l'application (2) et par la puce électronique.

Selon un autre mode particulier de mise en œuvre, la fonction non linéaire f a en outre comme arguments d'entrée au moins un paramètre c dépendant de l'état de la puce électronique au moment de l'authentification. Selon une première variante à ce mode, la valeur du paramètre c est calculée à partir d'au moins la valeur d'un compteur contenu dans la puce électronique et incrémenté à chaque authentification. Selon une seconde variante à ce mode, la valeur du paramètre c est calculée à partir, d'au moins la valeur d'un compteur contenu dans la puce électronique et incrémenté à chaque authentification et, de l'aléa R.

Selon un autre mode particulier de mise en œuvre, le masquage du certificat au moyen du masque M est calculé au moyen d'une fonction de chiffrement, en particulier une opération OU Exclusif bit à bit.

Selon un autre mode particulier de mise en œuvre, le nombre d'authentifications de la puce électronique est limité à une valeur maximale V déterminée par l'application et inscrite dans la puce électronique. Selon une variante à ce mode, la puce électronique contient un compteur incrémenté à chaque authentification et, la puce électronique cesse tout calcul d'authentification lorsque la valeur du compteur atteint la valeur maximale V.

D'autres caractéristiques et avantages de l'invention apparaîtront lors de la description qui suit faite en regard de dessins annexés de modes particuliers de réalisation donnés à titre d'exemples non limitatifs.

La figure 1 est un schéma d'un procédé selon l'invention.

La figure 2 est un schéma d'une fonction non linéaire f.

La figure 1 représente schématiquement un procédé selon l'invention, de protection d'une puce électronique 1 d'un utilisateur contre la fraude dans des transactions entre une application 2 et la puce électronique 1.

L'application 2 peut être entièrement ou partiellement délocalisée dans un terminal en libre service non surveillé, tel un téléphone public ou tel un tourniquet d'accès à un transport public. L'utilisateur détient une puce électronique 1, implantée par exemple sur une carte prépayée, qui doit lui permettre d'établir une transaction avec l'application 2. Ces transactions peuvent consister en l'établissement de communications téléphoniques, le paiement d'objets dans un distributeur automatique, la location d'emplacement de stationnement à partir d'un parcmètre, le paiement d'un service comme un transport public ou comme la mise à disposition d'infrastructures.

Le procédé permet d'authentifier la puce électronique 1. La puce électronique 1 est personnalisée au moment de sa fabrication et, éventuellement lors d'une opération

de rechargement, au moyen d'un numéro d'identité i et d'une valeur initiale d'une donnée D liée à l'application à laquelle elle est destinée ; la valeur D représente généralement le crédit attaché à la puce électronique 1 pour une application 2 donnée.

Le procédé consiste, lors de cette opération de personnalisation ou, lors d'une opération préalable à la commercialisation de la puce électronique 1, à déterminer les conditions initiales nécessaires à l'authentification, soit de la puce électronique 1, soit de l'application 2. Ces conditions initiales comprennent la détermination 3 d'une fonction logique g, d'une fonction non linéaire f, d'une première clé secrète K et d'une seconde clé secrète K'. La fonction logique g est connue de l'application 2 et est implantée dans la puce électronique 1 sous la forme de circuits logiques 4 tels des circuits « ou », « ou exclusif », « et », « non et », ...

La fonction non linéaire f peut être implantée sous la forme d'un circuit 5 formé d'une succession de registres formant un registre à décalage, associés à une mémoire et à des opérateurs ou exclusifs ; une telle fonction est dite « automate d'états » et un exemple est représenté à la figure 2. Suivant cet exemple, la fonction f consiste en un premier opérateur ou exclusif 6, un registre à décalage 4 bits comprenant quatre bascules r0 à r3 et quatre opérateurs ou exclusifs 7 à 10 et, en une mémoire 11 de taille 16x4 bits. Chaque opérateur ou exclusif 6 à 10 a deux entrées et une sortie. Chaque bascule r0 à r3 a une entrée de données, deux sorties de données et une entrée horloge non représentée. La mémoire 11 a quatre entrées et quatre sorties et une entrée horloge non représentée. Les arguments d'entrée e_5, e_6 qui comprennent, selon ce mode de réalisation, au moins une partie de la seconde clé secrète K' et l'aléa R sont présents sur une des entrées du premier opérateur ou exclusif 6. La sortie du premier opérateur ou exclusif 6 est connectée à la première entrée du deuxième opérateur ou exclusif 7. L'entrée des bascules r0, r1, r2 et r3 est connectée à la sortie d'un opérateur ou exclusif 7 à 10. La première sortie des bascules r0, r1 et r2 est connectée à une première entrée d'un opérateur ou exclusif 8 à 10. La seconde sortie des bascules r0, r1, r2 et r3 est connectée à une entrée de la mémoire 11. La seconde entrée des opérateurs ou exclusifs 7 à 10 est connectée à une sortie de la mémoire 11. La première sortie de la bascule r3 donne la valeur du masque M calculée par la fonction f appliquée aux arguments e_5, e_6 qui comprennent, selon ce mode de réalisation, au moins une partie de la seconde clé secrète K' et l'aléa R. A chaque authentification de la puce électronique 1 ou, de l'application 2, correspond un nombre de coups d'horloge égal au nombre de bits des arguments d'entrée ; les bits du masque M sortent en série à chaque coup d'horloge sur la sortie 12.

La première clé K, généralement attribuée de manière individuelle à une puce électronique, consiste typiquement en un mot de quelques dizaines à quelques milliers de bits ; ce mot est connu de l'application et est gardé secret dans la puce électronique 1. Cependant, selon un mode particulier de réalisation du procédé, l'application ne mémorise pas la clé K elle-même mais un secret dit maître. Ce secret maître est tel qu'il permet de reconstituer, par une méthode dite de diversification, la clé K à partir du numéro i d'identité de la puce.

Quel que soit le mode de réalisation du procédé, la clé K est typiquement conservée dans la puce dans une mémoire 13 morte telle une PROM. En particulier, lorsque la puce électronique 1 est de type rechargeable, c'est le cas d'une puce implantée sur une carte prépayée à rechargement, la mémoire morte est aussi accessible en écriture, telle une EEPROM.

La seconde clé K' se présente comme la clé K, sous la forme d'un mot d'un certain nombre de bits. Les clés K et K' sont mémorisées dans la puce, typiquement dans la même mémoire 13 à des adresses différentes, mais la détermination des bits de K' (respectivement K) peut, dans certains cas, dépendre de la clé K (respectivement K').

Après l'opération de personnalisation, la puce électronique 1 est commercialisée et l'utilisateur peut entreprendre une transaction avec une application 2. Le procédé d'authentification, illustré par le schéma de la figure 1, consiste à authentifier la puce électronique 1 par l'application 2.

Dans une première étape du procédé, l'application génère un mot R appelé aléa. Le mot R comprend un nombre de bits déterminé pour éviter toute tentative frauduleuse de rejeu ; typiquement le nombre de bits est de l'ordre de quelques dizaines de bits. Le mot R est généré à l'aide d'un générateur aléatoire ou d'un générateur pseudo aléatoire. Dans un mode particulier de réalisation, les mots R successivement générés peuvent consister en une suite d'entiers consécutifs. Le mot R est un argument d'entrée pour le calcul du certificat S. Pour que la puce électronique 1 ait accès au mot R, l'application 2 effectue une écriture 14 dans la puce 1 ou la puce 1 vient lire le mot R dans l'application 2. L'échange entre la puce 1 et l'application 2 peut s'effectuer suivant un protocole établi lors de la personnalisation de la puce 1 ; la valeur R peut, par exemple, être codée. Le mot R est stocké temporairement dans une mémoire tampon 15 de la puce électronique 1, ainsi que dans l'application 2.

Dans une deuxième étape du procédé, l'application 2 d'une part et, la puce 1 d'autre part, calculent 16, 17 un certificat noté respectivement S et Sp. Le certificat S,

respectivement Sp, est le résultat du calcul effectué par la fonction logique g appliquée à une liste d'arguments e_1, e_2 qui comprend au moins l'aléa R et la clé K. Dans des modes particuliers de réalisation du procédé, la liste d'arguments e_1, e_2 comprend en outre, le numéro i d'identité de la puce électronique 1 ou, une ou plusieurs données D contenues dans la puce électronique 1 ou, une ou plusieurs données D' générées par l'application et écrites dans la puce électronique 1 avant authentification ou, une combinaison des arguments précédents.

Dans une troisième étape, le procédé consiste à déterminer 18, 19 un masque M au moyen de la fonction non linéaire f. Le masque M est le résultat de la fonction non linéaire f appliquée à une liste d'arguments e_5, e_6 comme décrit ci-dessus en regard de la figure 2. Le masque M consiste en un nombre déterminé m de bits qui est typiquement égal à une dizaine de bits. Le mode de réalisation suivant lequel le nombre m est égal au nombre de bits du certificat S a pour avantage que le certificat masqué ne révèle strictement aucune information sur la valeur du certificat S ; ceci n'est pas le cas lorsque la longueur m du masque M est plus courte que la longueur du certificat S.

Dans une quatrième étape du procédé, la puce électronique 1 masque 20 la valeur du certificat Sp qu'elle a calculée au moyen du masque M. Dans un premier mode de réalisation, le masquage 20 est calculé au moyen d'une fonction de chiffrement. Une fonction de chiffrement est une fonction bijective paramétrée par une clé qui, à un ensemble de valeurs, fait correspondre un autre ensemble de valeurs ; par exemple la fonction F : $x \rightarrow x + k$ modulo 2, avec x=0 ou 1 et k = 0 ou 1, peut être utilisée comme fonction de chiffrement. La fonction de chiffrement peut consister en une opération ou exclusif entre le certificat Sp et le masque M. Le résultat de l'opération de masquage donne la valeur du certificat masquée Spm qui est stockée de manière temporaire dans une mémoire 21 tampon de la puce électronique 1.

Dans une cinquième étape du procédé, l'application effectue une lecture 22 de la mémoire 21 tampon ou la puce 1 vient écrire le certificat masqué Spm dans l'application 2. L'échange entre la puce 1 et l'application 2 peut s'effectuer suivant un protocole similaire à celui utilisé pour l'échange de l'aléa R. L'application 2 vérifie alors la valeur Spm du certificat masqué calculée par la puce 1 en la comparant 23 à la valeur S du certificat qu'elle a elle-même calculée. Pour effectuer la comparaison 23, soit, comme illustré, l'application 2 masque 24 la valeur S du certificat au moyen du masque M pour obtenir la valeur masquée Sm et la comparer 23 à la valeur Spm., soit

l'application 2 démasque la valeur Spm en faisant intervenir une fonction inverse du masque M pour obtenir la valeur Sp et la comparer à la valeur S.

Une variante du procédé précédemment décrit en regard des figures 1 et 2 permet avantageusement de remédier à certaines tentatives de fraude consistant à simuler vis à vis d'une puce électronique le comportement d'une application, à l'aide d'une authentification de l'application par la puce électronique. Selon cette variante, des opérations précédemment effectuées par l'application sont effectuées par la puce électronique et vice versa. Ainsi :

- à chaque authentification de l'application, le mot d'entrée variable R appelé aléa est généré, de préférence, par la puce électronique,
- l'application calcule un certificat et, le masque au moyen du masque M pour rendre disponible à la puce électronique uniquement la valeur du certificat masquée,
- l'opération de comparaison des valeurs de certificat calculées d'une part par la puce électronique et, d'autre part par l'application est effectuée par la puce électronique.

L'invention a en outre pour objet une puce électronique destinée à des transactions avec une application, les transactions mettant en œuvre un procédé selon l'invention. La puce comporte :

- une mémoire non volatile telle une PROM ou une EEPROM pour stocker la première clé secrète K et la seconde clé secrète K',
- un premier circuit électronique tel, un microprocesseur, un circuit logique programmable (EPLD ou PAL selon les terminologies anglo-saxonnes), pour calculer le certificat Sp et pour calculer le masque M,
- des circuits intégrés dans lesquels sont implantées la fonction logique g et la fonction non linéaire f,
- un second circuit électronique tel, un microprocesseur, un circuit logique programmable (EPLD ou PAL selon les terminologies anglo-saxonnes), pour masquer le certificat avec le masque M.

L'invention a en outre pour objet une carte prépayée comportant une telle puce électronique.

L'invention a en outre pour objet un dispositif destiné à des transactions avec de telles puces électroniques, les transactions mettant en œuvre un procédé selon l'invention. Le dispositif comporte :

- un moyen de mémorisation pour mémoriser les clés secrètes, K, K', des puces électroniques, la fonction logique g et la fonction non linéaire f,
- un moyen de calcul pour calculer le certificat S et pour calculer le masque M,
- un moyen de vérification pour vérifier la valeur masquée Spm du certificat calculé par une puce électronique.

Le dispositif est compris dans un équipement tel, un téléphone public, une borne d'accès à un service public (un tourniquet d'accès à un métro, un tourniquet d'accès à une bibliothèque,...), un parcmètre.

REVENDICATIONS

1. Procédé de protection d'une puce électronique (1) d'un utilisateur contre la fraude dans des transactions entre une application (1) et la puce électronique (2) comprenant les étapes consistant :

- à déterminer (3) une fonction logique g connue de l'application (2) et implantée (4) dans la puce électronique (1),
- à attribuer à la puce électronique (1) une première clé secrète K, connue seulement de la puce électronique (1) et de l'application (2), et gardée secrète (13) dans la puce électronique (1),
- à chaque authentification de la puce électronique (1) à générer un mot d'entrée variable R appelé aléa,
- à calculer (16, 17) un certificat (Sp, S), par la puce électronique (1) et l'application (2), le certificat (Sp, S) étant le résultat de la fonction logique g appliquée à une liste d'arguments (e_1, e_2) comprenant au moins l'aléa R et la clé secrète K, caractérisé en ce que ledit procédé comprend en outre les étapes consistant :
- à déterminer une fonction non linéaire f connue de l'application (2) et implantée dans la puce électronique (1),
- à attribuer à la puce électronique (1) une seconde clé secrète K' connue seulement de la puce électronique (1) et de l'application (2), et gardée secrète (13) dans la puce électronique (1),
- à chaque authentification de la puce électronique (1) à déterminer (18, 19) un masque M au moyen de la fonction non linéaire f appliquée à une liste d'arguments (e_5, e_6) comprenant au moins une partie de la clé secrète K',
- à masquer (20) la valeur du certificat (Sp) au moyen du masque M pour rendre disponible à l'application (2) uniquement la valeur du certificat masquée (Spm),
- à vérifier par l'application (2) la valeur masquée (Spm) du certificat calculée par la puce électronique (1).

2. Procédé selon la revendication 1, caractérisé en ce que la vérification par l'application (21) de la valeur masquée (Spm) du certificat calculée par la puce électronique (1) consiste :

- à démasquer au moyen du masque M la valeur masquée (Spm) du certificat calculée par la puce électronique (1) et,
- à comparer la valeur du certificat (Sp) calculée par la puce électronique (1) à celle (S) calculée par l'application (2).

3. Procédé selon la revendication 1, caractérisé en ce que la vérification par l'application (2) de la valeur masquée (Spm) du certificat calculée par la puce électronique (1) consiste :
   - à masquer (24) au moyen du masque M la valeur du certificat (S) calculée par l'application (2) et,
   - à comparer (23) la valeur masquée du certificat (Spm) calculée par la puce électronique (1) à la valeur masquée du certificat (Sm) calculée par l'application (2).

4. Procédé selon la revendication 1, caractérisé en ce que le masquage (20, 24) du certificat (Sp, S) au moyen du masque M est calculé au moyen d'une fonction de chiffrement.

5. Procédé selon la revendication 4, caractérisé en ce que la fonction de chiffrement est une opération OU Exclusif bit à bit.

6. Procédé selon la revendication 1, caractérisé en ce que l'aléa R est déterminé par l'application (2) à partir d'un nombre aléatoire généré par l'application (2) et en ce que l'aléa R est transmis à la puce électronique (1) par l'application (2).

7. Procédé selon la revendication 1, caractérisé en ce que l'aléa R est déterminé à partir d'une suite d'entiers consécutifs générés par l'application (2) et par la puce électronique (1).

8. Procédé selon la revendication 1, caractérisé en ce que le certificat (Sp, S) et le masque M ont le même nombre de bits.

9. Procédé selon la revendication 1, caractérisé en ce que le certificat (Sp, S) est le résultat de la fonction logique g appliquée à une liste d'arguments (e_1, e_2)

comprenant au moins l'aléa R, la clé secrète K et des données D internes à la puce électronique (1).

10. Procédé selon la revendication 1, caractérisé en ce que le certificat (Sp, S) est le résultat de la fonction logique g appliquée à une liste d'arguments (e_1, e_2) comprenant au moins l'aléa R, la clé secrète K et des données D' fournies à la puce électronique (1) par l'application (2) lors de l'authentification.

11. Procédé selon la revendication 1, caractérisé en ce que la clé secrète K consiste en une séquence de valeurs K[i] et, en ce que la fonction logique g déterminant la valeur du certificat (Sp, S) consiste en un calcul de produits scalaires modulo 2 entre chacune des valeurs K[i] et les arguments d'entrée autres que la clé K de la fonction logique g.

12. Procédé selon la revendication 1, caractérisé en ce que les clés secrètes K et K' sont choisies indépendamment l'une de l'autre.

13. Procédé selon la revendication 1, caractérisé en ce que la fonction non linéaire f a en outre comme arguments d'entrée au moins l'aléa R.

14. Procédé selon la revendication 1, caractérisé en ce que la fonction non linéaire f a en outre comme arguments d'entrée (e_5, e_6) au moins des données D internes à la puce électronique.

15. Procédé selon la revendication 1, caractérisé en ce que la fonction non linéaire f a en outre comme arguments d'entrée (e_5, e_6) au moins des données D' fournies à la puce électronique (1) par l'application (2).

16. Procédé selon la revendication 1, caractérisé en ce que la fonction non linéaire f a en outre comme arguments d'entrée (e_5, e_6) au moins un paramètre c dépendant de l'état de la puce électronique (1) au moment de l'authentification.

17. Procédé selon la revendication 16, caractérisé en ce que la valeur du paramètre c est calculée à partir d'au moins la valeur d'un compteur contenu dans la puce électronique (1) et incrémenté à chaque authentification.

18. Procédé selon la revendication 16, caractérisé en ce que la valeur du paramètre c est calculée à partir, d'au moins la valeur d'un compteur contenu dans la puce électronique (1) et incrémenté à chaque authentification et, de l'aléa R.

19. Procédé selon la revendication 1, caractérisé en ce que le nombre d'authentifications de la puce électronique (1) est limité à une valeur maximale V déterminée par l'application (2) et inscrite dans la puce électronique (1).

20. Procédé selon la revendication 14, caractérisé en ce que la puce électronique (1) contient un compteur incrémenté à chaque authentification, et que la puce électronique (1) cesse tout calcul d'authentification lorsque la valeur du compteur atteint la valeur maximale V.

21. Procédé de protection d'une puce électronique (1) d'un utilisateur contre la fraude dans des transactions entre une application (2) et la puce électronique (1) comprenant les étapes consistant :

- à déterminer une fonction logique g connue de l'application (2) et implantée (4) dans la puce électronique (1),
- à attribuer à la puce électronique (1) une première clé secrète K, connue seulement de la puce électronique (1) et de l'application (2), et gardée secrète (13) dans la puce électronique (1),
- à chaque authentification de l'application (2) à générer un mot d'entrée variable R appelé aléa,
- à calculer un certificat (Sp, S), par la puce électronique (1) et l'application (2), le certificat (Sp, S) étant le résultat de la fonction logique g appliquée à une liste d'arguments (e_1, e_2) comprenant au moins l'aléa R et la clé secrète K, caractérisé en ce que ledit procédé comprend en outre les étapes consistant :
- à déterminer une fonction non linéaire f connue de l'application (2) et implantée dans la puce électronique (1),
- à attribuer à la puce électronique (1) une seconde clé secrète K', connue seulement de la puce électronique (1) et de l'application (2), et gardée secrète (13) dans la puce électronique (1),

- à chaque authentification de l'application (2) à déterminer (18, 19) un masque M calculé au moyen de la fonction non linéaire f appliquée à au moins une partie de la clé secrète K',
- à masquer la valeur du certificat (S) au moyen du masque M pour rendre disponible à la puce électronique (1) uniquement la valeur du certificat (Sm) masquée,
- à vérifier par la puce électronique (1) la valeur masquée du certificat (Sm) calculée par l'application (2).

22. Procédé selon la revendication 21, caractérisé en ce que l'aléa R est déterminé par la puce électronique (1) à partir d'un nombre aléatoire généré par la puce électronique (1) et en ce que l'aléa R est transmis à l'application (2) par la puce électronique (1).

23. Procédé selon la revendication 21, caractérisé en ce que l'aléa R est déterminé à partir d'une suite d'entiers consécutifs générés par l'application (2) et par la puce électronique (1).

24. Puce électronique (1) destinée à des transactions avec une application (2), les transactions mettant en œuvre un procédé selon l'une des revendications 1 à 20, caractérisée en ce qu'elle comporte :
- un moyen de mémorisation (13) pour stocker la première clé secrète K et la seconde clé secrète K',
- un moyen de calcul (16,18) pour calculer le certificat (Sp) et pour calculer le masque M,
- un moyen électronique (4, 5) dans lequel sont implantées la fonction logique g et la fonction non linéaire f,
- un moyen de masquage (20) pour masquer le certificat avec le masque M.

25. Puce électronique (1) selon la revendication 24, caractérisée en ce qu'elle comporte en outre :
- un moyen de comptage du nombre d'authentifications de la puce électronique (1) pour une application donnée (2) pour contrôler la durée d'utilisation de la puce électronique (1).

26. Carte prépayée comportant une puce électronique (1) selon la revendication 24.

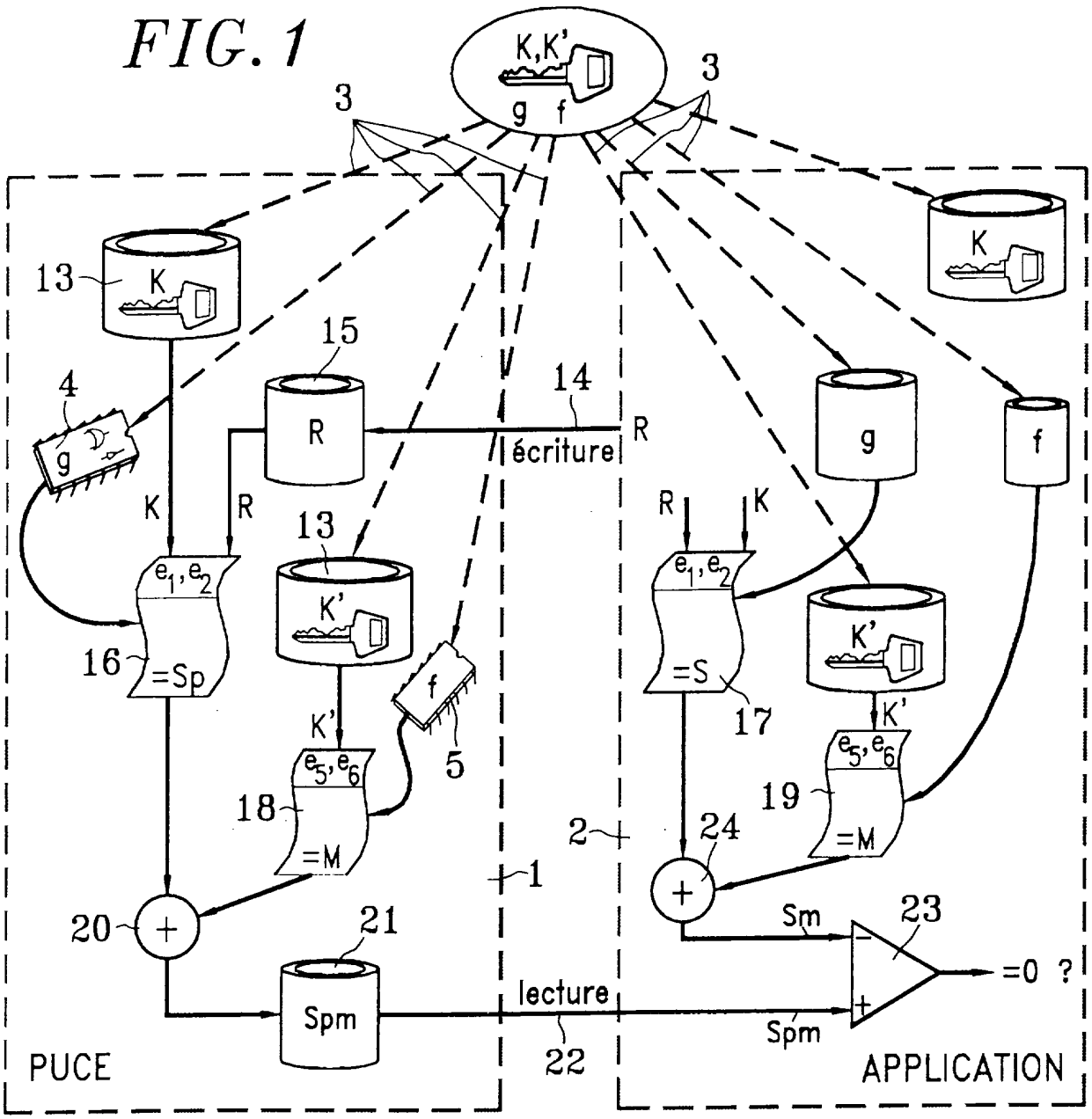
27. Dispositif destiné à des transactions avec des puces électroniques (1), les transactions mettant en œuvre un procédé selon l'une des revendications 1 à 20, caractérisé en ce qu'il comporte :
    - un moyen de mémorisation pour mémoriser les clés secrètes, K, K', des puces électroniques, la fonction logique g et la fonction non linéaire f,
    - un moyen de calcul pour calculer le certificat (S) et pour calculer le masque M,
    - un moyen de vérification pour vérifier la valeur masquée (Spm) du certificat calculé par une puce électronique (1).

28. Téléphone public comportant un dispositif selon la revendication 27.

29. Borne d'accès à un service public comportant un dispositif selon la revendication 27.

30. Parcmètre comportant un dispositif selon la revendication 27.

FIG. 1


K,K'
g
f
3
3
13
K
15
R
14
écriture
R
4
g
K
R
13
K'
e1, e2
16
=Sp
K'
e5, e6
18
=M
f
5
1
2
R
K
e1, e2
=S
17
g
f
K
K'
K'
e5, e6
19
=M
24
20
21
Sm
23
=0 ?
Spm
lecture
Spm
22
PUCE
APPLICATION

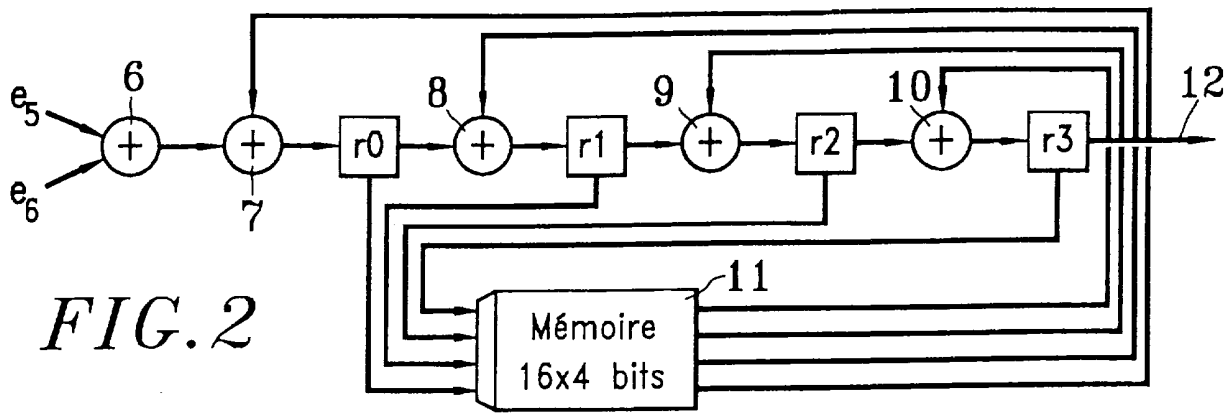

e5
e6
6
7
r0
8
r1
9
r2
10
r3
12
11
Mémoire
16x4 bits

FIG. 2

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2807245

N° d'enregistrement national

FA 584725
FR 0004313

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	WO 97 22093 A (LANDIS & GYR) 19 juin 1997 (1997-06-19) * abrégé; revendications; figure 1 * * page 2, ligne 25 - page 3, ligne 28 * ---	1,3-6,8, 9,13,14, 21,24, 26-29	H04L9/28 G06K19/073 G07F7/12
A	EP 0 565 279 A (AMERICAN TELEPHONE AND TELEGRAPH) 13 octobre 1993 (1993-10-13) * abrégé; revendications; figure 5 * * page 5, ligne 9 - ligne 33 * ---	1,2,6,9, 21,24, 26-28	
A	EP 0 621 570 A (FRANCE TELECOM)) 26 octobre 1994 (1994-10-26) * le document en entier * ---	1,6,9, 10, 16-18, 21,24-27	
A	DE 41 38 861 A (SIEMENS NIXDORF INFORMATIONSSYSTEME) 1 octobre 1992 (1992-10-01) * le document en entier * -----	1,6,9, 10,21,22	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G07F H04L

Date d'achèvement de la recherche	Examinateur
18 janvier 2001	David, J

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet 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 12.99 (P04C14)