(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 620 248**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **87 12366**

(51) Int Cl⁴ : G 06 K 9/62, 19/00.

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 7 septembre 1987.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 10 du 10 mars 1989.

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

(71) **Demandeur(s) :** *ETAT FRANCAIS, représenté par le Ministre délégué des Postes et Télécommunications, Centre National d'Etudes des Télécommunications, Etablissement Public de diffusion dit : TELEDIFFUSION DE FRANCE.* — FR et *PHILIPS S.A., Laboratoire de Recherches Bruxelles.* — BE.

(72) **Inventeur(s) :** Louis C. Guillou ; Jean-Jacques Quisquater.

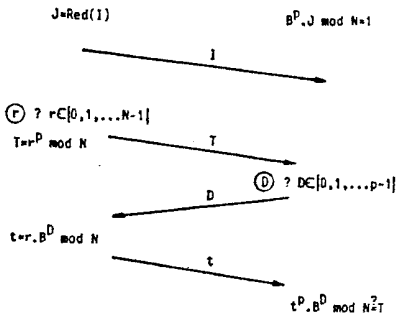
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** Brevatome.

## (54) Procédés d'authentification d'accréditations ou de messages à apport nul de connaissance et de signature de messages.

(57) Au lieu d'utiliser des accréditations multiples et un processus itératif de vérification, on utilise une accréditation profonde (exposant $p$ élevé) et on tire au hasard un nombre D compris entre 0 et $p-1$. Les opérations de vérification passent par le calcul de la puissance D ième de l'accréditation inverse B.

Application notamment aux cartes à puce et plus spécialement aux cartes bancaires.




FR 2 620 248 - A1

2620248

# PROCEDES D'AUTHENTIFICATION D'ACCREDITATIONS OU DE MESSAGES A APPORT NUL DE CONNAISSANCE ET DE SIGNATURE DE MESSAGES

## DESCRIPTION

La présente invention a pour objet des procédés d'authentification d'accréditations ou de messages à apport nul de connaissance et un procédé de signature de messages.

L'invention trouve de nombreuses applications dans la vérification de l'authenticité de cartes bancaires dites "à puces" ou plus généralement de l'authenticité de tout support permettant à son détenteur de commander un accès, (à un local, à un coffre, à une banque de données, à un système informatisé, à une ligne téléphonique, etc...). Elle s'applique également à la vérification de l'authenticité de messages de toute nature, ces messages pouvant commander une ouverture ou une fermeture, l'enclenchement ou l'arrêt d'un système, la commande de la mise à feu d'un engin, la commande d'un satellite, le déclenchement d'une alerte etc... Enfin, l'invention permet de signer des messages de telle manière que leurs destinataires soient assurés de leur provenance, et puissent à leur tour convaincre un tiers sur cette provenance.

L'invention s'appuye sur deux branches de la cryptographie qui sont respectivement la cryptographie à clé révélée (ou à clé publique) et les procédures de vérification à apport nul de connaissance. Bien que l'invention ne concerne pas un procédé de chiffrement, il n'est pas inutile de rappeler en quoi consistent ces deux techniques.

De tout temps le maintien du secret des communications a été une préoccupation. Aujourd'hui que les systèmes de télécommunications prolifèrent, il est devenu un problème majeur. De ce fait, les techniques de chiffrement et de déchiffrement ont progressé considérablement ces dernières années. Ce progrès a d'ailleurs été encore accéléré par l'avènement des calculateurs,

qui ont permis d'élaborer des cryptosystèmes à hautes performances.

Dans un cryptosystème, un message M, dit message en clair, est transformé à l'aide d'une clé E, pour donner un message E(M) dit message chiffré. A la clé E correspond une clé inverse D qui permet de retrouver le message en clair par une transformation inverse : D(E(M))=M.

Dans les techniques traditionnelles les deux clés E et D sont tenues secrètes et ne sont connues que des seuls interlocuteurs.

Cependant, un cryptosystème original a été developpé ces dernières années, dans lequel la clé de chiffrement n'est plus tenue secrète mais est, au contraire, révélée. Paradoxalement, cette révélation n'affaiblit en rien la sécurité du système. En effet, il se trouve que le chiffrement utilise une fonction telle que la connaissance de la clé E ne permet pas, dans la pratique, de retrouver la clé D de déchiffrement. On parle alors, de manière imagée, d'une fonction "trappe" pour la fonction de chiffrement, fonction qui est particulièrement difficile à inverser, sauf pour celui qui connaît la valeur de la trappe.

Les principes généraux de ces systèmes ont été décrits dans l'article de W. DIFFIE et M. HELLMANN intitulé "New Directions in Cryptography" publié dans IEEE, Transactions ou Information Theory, vol. IT-22, pp 644-654, Nov. 1976.

On peut aussi consulter à ce sujet l'article de M. HELLMAN intitulé "The Mathematics of Public-Key Cryptography" publié dans Scientific American d'Août 1979, vol.241, n°2, pp 130-139 ou sa traduction française dans l'édition de "Pour la Science" sous le titre "Les Mathématiques de la Cryptographie à clef révélée", Octobre 1979, vol. n°24, pp 114-123.

Les principes théoriques de la cryptographie à clé révélée ont pu être mis en application de manière particulièrement efficace dans un système dit RSA (des initiales de ses inventeurs Ronald RIVEST - Adi SHAMIR et Léonard ADLEMAN).

Ce système est décrit dans l'article de Martin GARDNER intitulé "A new kind of cipher that would take millions of year to break" publié dans Scientific American, Août 1977, pp. 120-121. Dans le système RSA la fonction trappe est la factorisation d'un nombre en éléments premiers. On sait que l'opération de factorisation est l'une des plus difficiles de l'arithmétique. Par exemple pour trouver, à la main, les facteurs premiers d'un nombre modeste à 5 chiffres comme 29 083, il faut quelques minutes. Ces nombres sont 127 et 229. Mais l'obtention du produit de 127 par 229 ne prend que quelques secondes. L'asymétrie d'une telle opération est donc flagrante. Naturellement, le recours à un ordinateur accélère la factorisation mais il demeure que, pour factoriser un nombre de deux cents chiffres, même en mettant ensemble les ordinateurs les plus puissants ordinateurs.

En pratique donc, on ne sait pas factoriser un très grand nombre.

Ces propriétés sont exploitées dans le système RSA de la manière suivante. On choisit deux nombres premiers distincts, soit a et b, et on en forme le produit, soit N=a.b. On choisit également un entier p, qui est premier avec le plus petit commun multiple de (a-1) et (b-1). Pour chiffrer un message, préalablement mis sous forme numérique M, M étant compris entre 0 et N-1, on calcule la puissance pième de M dans l'anneau des entiers modulo N, soit $C=M^p$ mod N. (On rappelle que la valeur d'un entier x modulo un entier y est égale au reste de la division de x par y ; ainsi, 27 modulo 11 est égal à 5, car 27 divisé par 11 donne 5 comme reste). La fonction "élever à la puissance p modulo N" définit alors une permutation des entiers de 0 à N-1.

Pour déchiffrer un message tel que C il faut extraire la racine pième du message chiffré C dans l'anneau des entiers modulo N. On montre que cette opération revient à élever le nombre C à la puissance d, d étant l'inverse de l'exposant p modulo le plus petit commun multiple des nombres (a-1) et (b-1). Si l'on ne connait pas les facteurs premiers a et b, la

détermination de d est impossible et avec elle, l'opération de déchiffrement.

Par exemple, en choisissant a=47 et b=59, on obtient N=47.59=2773. On peut prendre p=17. La clé de codage est donc définie par les deux nombres 2773 et 17 (naturellement, dans la pratique, les nombres utilisés sont beaucoup plus grands que dans cet exemple).

Le codage d'un mot M se présentant sous forme du nombre 920 s'effectue par l'opération suivante :

$$C = 920^{17} \bmod 2773$$

soit $C = 948 \bmod 2773$.

Inversement, pour déchiffrer le nombre 948, on utilisera un exposant d inverse de 17 modulo 1334 qui est le ppcm de 46 et 58. Cet exposant d est 157 car 157.17=2669 soit 1 modulo 1334. Déchiffrer 948 revient donc à calculer $948^{157}$ mod 2773 soit 920, ce qui est bien le message initial.

Ainsi, dans le système RSA, les nombres N et p peuvent ils être publics (on parle alors de la "puissance publique p"), mais les nombres a et b doivent rester secrets.

Naturellement, il est toujours possible d'utiliser plus de deux facteurs premiers pour constituer le nombre N.

Le système RSA est décrit dans le brevet des Etats-Unis d'Amérique n°4,405,829 délivré le 20 Septembre 1983.

Un tel système peut non seulement servir à chiffrer mais aussi à signer un message.

Dans le contexte de la signature de messages une entité censée émettre des messages M, entité appelée signataire, est réputée travailler avec une clé publique (N, p). Cette entité, pour signer ses messages avant émission, y ajoute une redondance pour obtenir un élément de l'anneau des entiers modulo N, puis élève cet élément à la puissance d (inverse de p) modulo N. L'entité en question, détenant les paramètres secrets de la clé publique, c'est-à-dire les deux facteurs premiers a et b, connait d. Le message signé est donc $S = \left[\text{Red}(M)\right]^{d} \bmod N$.

Pour vérifier la signature, le destinataire du message

utilise la clé publique (N, p) attachée à l'entité émettrice et calcule $S^p$ mod N, ce qui, par hypothèse redonne l'élément codant le message M avec sa redondance. En retrouvant la redondance le destinataire en conclut ainsi que le message n'a pu être envoyé que par l'entité qui prétend l'avoir fait, puisque seule, celle-ci, était capable de traiter le message de cette manière.

Naturellement, les deux opérations de chiffrement et de signature peuvent se combiner. Dans ce cas, l'émetteur commence par signer son message en utilisant sa clé secrète ; puis il le chiffre en utilisant la clé publique de son correspondant. A la réception, le correspondant déchiffre le message à l'aide de sa clé secrète, puis authentifie le message en utilisant la clé publique de l'émetteur.

Ces techniques de cryptographie conduisent ainsi à des méthodes d'authentification (d'un support, d'un message, etc...). Pour exposer plus en détail cet aspect, qui est au coeur de l'invention, on prendra comme exemple l'authentification des cartes bancaires dites "à puce", sans que cela constitue naturellement en quoi que ce soit une limitation de la portée de l'invention. Le procédé décrit ci-après est utilisé dans les cartes bancaires à puce émises aujourd'hui en France et en Norvège, la généralisation des puces dans les cartes bancaires est en cours dans ces deux pays.

Une carte bancaire à puce possède une identité, qui est constituée par un enchaînement d'informations telles que le numéro de série de la puce, le numéro du compte bancaire, une période de validité et un code d'usage. La carte peut donner, sur demande, ces informations d'identité, qui se présentent sous forme d'une suite de bits formant un mot I.

A l'aide de règles de redondance, on peut constituer un nombre J deux fois plus long que I qu'on notera par la suite Red(I)=J. Par exemple, si le nombre I s'écrit sous forme de quartets, chaque quartet peut être complété par un quartet de redondance de manière à former autant d'octets de type à codage de HAMMING. Le nombre J est appelé souvent l'identité "ombragée"

(l'ombre étant constituée en quelque sorte par la redondance qui accompagne l'identité).

L'Organisation Internationale de Normalisation (ISO) a précisé ces questions dans la note ISO/TC97/SC20/N207 intitulée "Digital Signature with Shadow" devenue avant projet de norme DP9796.

L'autorité habilitée à délivrer de telles cartes, en l'occurrence la banque, choisit un système à clé publique (N, p). Elle publie les nombres N et p mais garde secrète la factorisation de N. L'identité ombragée J de chaque carte est alors considérée comme un élément de l'anneau des entiers modulo N. La banque peut en extraire la racine p ième dans cet anneau (ce qui, comme exposé plus haut, nécessite la connaissance des facteurs premiers de N, ce qui est le cas). Ce nombre, noté par la suite A, est en quelle que sorte l'identité de la carte signée par la banque. On l'appelle "accréditation". On a donc par définition $A=J^{1/p} \bmod N$.

Authentifier une accréditation revient alors à lire l'identité de la carte, soit sous la forme simple I, soit sous la forme ombragée J, puis à lire l'accréditation A dans la carte, à élever celle-ci à la puissance p dans l'anneau des entiers modulo N (ce qui est possible puisque les paramètres N et p sont connus) et à comparer enfin le résultat, soit $A^p \bmod N$, à J. Si $A^p \bmod N$ est égal à J alors l'accréditation A est authentique.

Si cette méthode permet de détecter des fausses cartes dont les identités auraient été élaborées de manière fantaisiste, elle présente néanmoins un inconvénient qui est celui de révéler l'accréditation des cartes authentiques. Un vérificateur peu scrupuleux pourrait donc reproduire des cartes identiques à celle qu'il vient de vérifier (cartes que l'on pourrait appeler des "clones") en reproduisant l'accréditation qu'il a lue dans la carte authentique.

Or, l'authentification d'une accréditation ne requiert pas, en toute rigueur, la communication de celle-ci au vérificateur, mais seulement l'établissement d'une conviction que

la carte dispose d'une accréditation authentique. Le problème est donc finalement de démontrer que la carte détient une accréditation authentique, sans révéler celle-ci.

Ce problème, qui semble insoluble à première vue, peut cependant être résolu par une procédure dite de preuve par apport nul de connaissance ("zero-knowledge proof"). Dans une telle procédure, l'entité qui tente d'apporter la preuve (et que l'on appellera par la suite le "vérifié") et l'entité qui attend cette preuve (et qu'on appellera le "vérificateur") adoptent un comportement interactif et probabiliste.

Cette technique à été décrite par Shafi GOLDWASSER, Silvio MICALI et Charles RACKOFF dans leur communication au "17th ACM Symposium on Theory of Computing" qui s'est tenu en Mai 1985, communication intitulée "The Knowledge Complexity of Interactive Proof Systems" et publiée dans les Comptes Rendus pp.291-304. Les premiers exemples ont été trouvés en théorie des graphes.

Adi SHAMIR a pensé le premier à utiliser ce procédé en théorie des nombres et on pourrait l'appliquer aux cartes à puces de la manière suivante. Ce procédé, que l'on appellera par la suite procédé S, est le suivant.

Au début de la transaction d'authentification, la carte proclame son identité I. Les règles de redondance connues de tous, permettent de déduire J, deux fois plus long que I, qui correspond à l'identité ombragée. La carte et le vérificateur connaissent tous deux les nombres N et p publiés par l'émetteur de cartes, mais seul ce dernier dispose de la factorisation du nombre N, qui est l'information de trappe utilisée pour calculer les accréditations.

La transaction d'authentification se poursuit en répétant le traitement suivant :

- la carte tire au hasard un élément r de l'anneau des entiers modulo N, en calcule la puissance p ième ($r^p$ mod N) dans l'anneau, et transmet cette puissance au vérificateur en guise de titre T pour l'itération ;

- le vérificateur tire au hasard un bit d (0 ou 1) (ou

si l'on veut, tire à pile ou face) pour demander à la carte en guise de témoin t : pour pile l'élément r, et pour face le produit de l'élément r par l'accrédition dans l'anneau (r.A mod N) ; autrement dit, dans l'incertitude du tirage le vérifié doit tenir disponible r et r.A mod N ce qui implique la connaissance de A ;

- le vérificateur élève le témoin t à la puissance p modulo N pour retrouver : pour pile, le test T, et pour face le produit dans l'anneau du titre T par l'identité ombragée J.

Ainsi, d'une part, il faut disposer de l'accréditation A pour posséder simultanément les deux valeurs possibles du témoin t, soit r et rA. D'autre part, le vérifié ne peut déduire de cette transaction la valeur A de l'accréditation car, même s'il demande au vérifié de lui fournir rA, il ne connaît pas r, qui a été tiré au hasard par le vérifié (le vérificateur connaît bien $r^p$, fourni comme titre par le vérifié, mais il est incapable d'en extraire la racine p ième modulo N, puisqu'il ne connaît pas la factorisation de N).

Le vérifié qui ne serait pas détenteur d'une accréditation authentique pourrait bluffer en tentant de deviner le tirage du vérificateur. S'il parie sur "0" ("pile") il estime que le vérificateur élèvera le titre à la puissance p modulo N et que le vérificateur comparera le résultat obtenu au titre T. Pour convaincre le vérificateur, le vérifié devra fournir comme titre T le témoin élevé à la puissance p. Si le bluffeur parie au contraire sur "1" ("face") il estime que le vérificateur élèvera le titre à la puissance p et multipliera ensuite le résultat obtenu par J. Il lui faut donc, pour convaincre, transmettre comme titre T, le témoin élevé à la puissance p multiplié par J.

Autrement dit, le vérifié a une chance sur deux de donner une bonne réponse s'il renverse la chronologie des événements, c'est-à-dire s'il détermine non pas d'abord le titre T puis le témoin t, mais s'il parie sur le tirage du vérificateur et s'il constitue le titre a posteriori à l'aide d'un témoin tiré au hasard.

Dans ce processus probabiliste, les chances du vérifié de deviner la bonne réponse sont de une sur deux à chaque traitement, de sorte qu'en répétant ce traitement k fois, les chances du bluffeur tombent à $1/2^k$. Le facteur de sécurité de ce procédé d'authentification est donc de $2^k$. En pratique, k est de l'ordre de 16 à 24.

Dans un tel procédé le nombre p est petit, par exemple 3. On peut aussi utiliser 2, mais dans ce cas certaines précautions doivent être prises dans le choix des facteurs premiers du nombre N pour que la fonction "élever au carré modulo N" soit une permutation sur les résidus quadratiques de l'anneau des entiers modulo N. Les nombres a et b doivent être des entiers de la forme 4x+3 ; on rappelle que les résidus quadratiques sont des éléments qui sont des carrés dans l'anneau et l'identité ombragée J doit pouvoir être modifiée en un résidu quadratique représentatif avant de calculer l'accréditation. Cette solution est décrite dans le document déjà cité ISO/TC97/SC20/N207. D'autres solutions existent cependant.

L'entier N, comme dans les cartes bancaires aujourd'hui, peut être de la forme $N=K+2^{320}$ où K est un entier de 240 bits publié et connu de tous les terminaux. Seul l'émetteur de cartes dispose de la factorisation de N. Il est tout de même conseillé de prendre des nombres composés plus grand.

L'identité I, comme dans les cartes bancaires aujourd'hui, peut être un motif de 160 bits, obtenu par le chaînage d'un numéro de série de la puce de 44 bits, d'un numéro de compte bancaire de 76 bits, d'un code d'usage de 8 bits et d'une période de validité de 32 bits. L'identité ombragée présente alors 320 bits. L'accréditation est alors la racine cubique de ce mot, modulo N. C'est un nombre de 320 bits.

Un perfectionnement de cette technique consiste à utiliser non pas l'accréditation elle-même A ($A^p \bmod N=J$) mais son inverse, noté B. On a alors $B^p J \bmod N=1$ ce qui permet de simplifier la comparaison du titre et du témoin. En effet, il suffit alors de transmettre un témoin égal à r(dB-d+1) (qui est

égal soit à r si d=0 soit à rB si d=1 et de calculer $t^{p(dJ-d+1)}$ mod N pour trouver le titre T. Ce dernier peut alors n'être transmis que partiellement, par exemple sous forme d'une centaine de ses bits ou encore mieux après une compression par une fonction à sens unique.

On rappelle qu'une fonction de compression fait correspondre à un ensemble de n éléments un ensemble de m autres éléments, m étant inférieur à n et tel qu'il sont pratiquement impossible de localiser deux éléments ayant même image.

La figure 1 annexée à la description illustre ce procédé. Les flèches allant de gauche à droite représentent une transmission du vérifié vers le vérificateur (identité I, titre T, témoin t) et les flèches allant de droite à gauche une transmission dans le sens inverse (bit d tiré au hasard). Un tirage au hasard est représenté par un cercle associé à un point d'interrogation. Le signe $\in$ signifie "appartient à" et les nombres entre accolades désignent l'ensemble des entiers compris entre les deux bornes indiquées, bornes comprises. La comparaison finale décidant de l'authenticité de l'accréditation est schématisée par un signe égal surmonté d'un point d'interrogation. Le tireté marque un ensemble d'opérations effectuées k fois (itération).

Il a été proposé récemment un procédé encore plus perfectionné, qui utilise des accréditations multiples. Ce procédé a été décrit dans la communication de Amos FIAT et Adi SHAMIR, publiée dans le Compte Rendu de CRYPTO' 86, Santa Barbara, CA, USA, August 1986, communication intitulée : "How to Prove Yourself : Practical Solutions to Identification and Signature Problems", Springer Verlag, lecture Notes in Computer Science, N°263, pp.186-194.

En notant dans la carte plusieurs accréditations, on augmente l'efficacité du traitement, et on réduit le nombre d'itérations nécessaires pour atteindre un niveau donné de sécurité vis-à-vis de la chance laissée au bluffeur. Dans cette méthode de diversification, on produit n identités diversifiées

I1, ..., In qui, complétées par leurs ombres, donnent n identités diversifiées ombragées J1, ..., Jn. La carte contient les n accréditations inverses B1, ..., Bn qui vérifient les relations $Ji.Bi^p \bmod N=1$.

Dans ce procédé, que l'on notera FS, chaque traitement ou itération devient alors le suivant (en prenant 2 pour exposant public) :

- la carte tire au hasard un élément r dans l'anneau des entiers modulo N, puis transmet au vérificateur 128 bits du carré de cet élément en guide de titre T ;

- le vérificateur tire au hasard un mot de n bits soit b1, ..., bn, qu'il transmet à la carte ;

- la carte calcule alors le produit de l'élément r par les accréditations inverses désignées par les bits à "1" dans le mots de n bits b1, ..., bn. Et la carte transmet en guise de témoin la valeur t ainsi obtenue :

$$t=r.(b1.B1-b1+1). \ldots .(bn.Bn-bn+1) \bmod N$$

- le vérificateur teste ce témoin t en l'élevant au carré dans l'anneau, puis en multipliant ce carré par les identités ombragées diversifiées désignées par les bits à "1" du mot de n bits,

soit : $t^p.(b1.J1-b1+1). \ldots .(bn.Jn-bn+1) \bmod N$

L'authenticité est prouvée si l'on retrouve les bits publiés du titre T.

N'importe qui pourrait tirer au hasard un témoin t, puis, dans l'anneau, élever au carré ce titre et multiplier par une sélection d'identités diversifiées pour constituer après coup un titre T. En effet, en donnant ce titre au début du traitement, si la question posée est bien la sélection escomptée, alors le témoin t est une réponse acceptable qui authentifie la carte.

Il y a donc bien une statégie gagnante pour le devin qui connaît à l'avance le tirage du vérificateur.

Pour passer avec succès une itération, le bluffeur doit, cette fois, deviner un mot de n bits et non plus un seul bit comme dans le procédé GMR. Si les $2^n$ valeurs sont

équiprobables, le produit de la multiplicité des accréditations (n) par le nombre des itérations (k) réduit exponentiellement les chances laissées au bluffeur. Le facteur de sécurité de la transaction d'authentification est alors $2^{k.n}$.

A chaque itération, le vérifié transmet par exemple 128 bits (par exemple un quart des 512 bits) et un élément de l'anneau, et le vérificateur transmet n bits. A chaque itération, le vérificateur et la carte calculent un carré et font un nombre de multiplications égal au nombre de bits à "1" dans le mot de n bits (poids de HAMMING).

Comme autre compromis entre efficacité de l'itération et nombre maximum de multiplications à effectuer durant l'itération on peut limiter le nombre de bits à 1 dans le mot de n bits.

On pourra consulter à propos de cette technique, le compte rendu de la communication de Amos FIAT et Adi SHAMIR au "5e Congrès Mondial de la Protection et de la Sécurité Informatique et des Communications" qui s'est tenu à Paris les 4-6 Mars 1987 sous le titre "Unforgeable Proofs of Identity".

La figure 2 annexée illustre schématiquement ce procédé FS, avec les mêmes conventions que pour la figure 1.

Ces procédés d'authentification d'accréditation peuvent se transposer aisément à l'authentification d'un message émis par une' entité censée être accréditée. Dans ce cas, le titre T transmis par le vérifié n'est plus formé uniquement par $r^p \bmod N$, comme dans le cas précédent, mais aussi par le message m à authentifier. Plus précisément, le résultat par une fonction de compression, notée f, dont les arguments sont m et $r^p \bmod N$.

Les figures 3 et 4 schématisent ces procédés dans le cas des techniques S et FS.

Enfin, ces techniques peuvent également servir à signer un message. La fonction de compression joue alors le rôle assigné au tirage du vérificateur. Plus précisément, dans le procédé de type S, le signataire tire k éléments r dans l'anneau des entiers modulo N, soit r1, r2, ..., rk, qui vont jouer le rôle des

différents r tirés au cours des k itérations. Le signataire élève ces entiers au carré mod N et calcule la fonction de compression $f(m, r^2 \bmod N, \ldots rk^2 \bmod N)$ ce qui fournit un nombre D ayant pour bits d1, d2, ..., dk. Chaque bit di de ce nombre joue le rôle que jouait le bit tiré au hasard dans le procédé d'authentification d'accréditation décrit plus haut. Le signataire forme alors k titres $ti=riB^{di} \bmod N$, avec i=1,2...k. Le message signé est alors constitué par un multiplet formé par m, I, d1, ..., dk, t1, ..., tk.

Pour vérifier un tel message signé on élève au carré les titres ti modulo N et on multiplie chaque carré par $J^{di}$ modulo N. On calcule ensuite la fonction de compression $f(m, t1^2 J^{d1} \bmod N, \ldots, tk^2 J^{dk} \bmod N)$ et l'on compare le résultat obtenu avec le nombre D, soit avec les bits d1, d2, ..., dk.

Dans l'application à la signature de messages, le nombre k est plus grand que dans l'authentification. Il est de l'ordre de 60 à 80. En effet, la vérification ne s'effectue plus en temps réel et le fraudeur a donc tout son temps pour élaborer une fausse signature.

Les figures 5 et 6 schématisent ce procédé dans le cas des techniques S et FS. Si toutes ces techniques de l'art antérieur conviennent bien en théorie, elles présentent cependant des inconvénients du point de vue pratique. En particulier, la méthode FS, avec la multiplicité de ses accréditations, consomme un espace mémoire important. Par ailleurs, la nécessité d'effectuer une répétition des traitements allonge la durée des échanges. Enfin, la multiplicité des témoins allonge les informations a ajouter à un message pour le signer.

La présente invention a justement pour but de remédier à cet inconvénient. A cette fin elle préconise une technique utilisant une seule accréditation (et non plus des accréditations multiples) et un seul traitement (et non plus une répétition de traitements).

De façon plus précise, la présente invention a d'abord pour objets un procédé d'authentification d'une accréditation et

un procédé d'authentification d'un message, procédés qui mettent tous deux en oeuvre, d'une part, l'élaboration d'une accréditation basée sur le système à clé publique et, d'autre part, une preuve à apport nul de connaissance ;

a) pour ce qui est de l'opération d'élaboration de l'accréditation, elle comprend les opérations connues suivantes :

- une autorité habilitée à délivrer des accréditations choisit deux nombres premiers, forme le produit (N) de ces deux nombres, tient secrets ces nombres qui constituent alors les facteurs premiers de N, choisit un entier p et publie N et p;

- pour chaque détenteur d'une accréditation, une identité numérique I est constituée, puis complétée par redondance pour former un mot J appelé identité ombragée,

- une accréditation A est élaborée par l'autorité en prenant la racine pième de l'identité ombragée dans l'anneau des entiers modulo N, ($A^p$ mod N=J),

- dans un support approprié contenant une mémoire, l'autorité charge l'inverse modulo N de l'accréditation A, soit un nombre B appelé accréditation inverse ($B^n$ J mod N=1), ce nombre B constituant l'accréditation qu'il s'agit d'authentifier ;

b) pour ce qui est de l'authentification de l'accréditation ainsi élaborée, cette opération consiste, de manière elle aussi connue, en un processus numérique interactif et probabiliste du type à apport nul de connaissance et s'établissant entre un support contenant une accréditation, support appelé "le vérifié" et un organe d'authentification appelé "le vérificateur", ce processus comprenant au moins un traitement numérique constitué par les opérations connues suivantes :

- le vérifié tire d'abord au hasard un entier r appartenant à l'anneau des entiers modulo N,

- le vérifié élève cet entier r à la puissance p modulo N, le résultat étant appelé titre T,

- le vérifié délivre alors au moins une partie des bits du titre T,

- le vérificateur tire ensuite au hasard un nombre D et demande au vérifié d'effectuer certaines opérations sur r et sur l'accréditation inverse B, ces opérations étant liées au nombre D tiré au hasard par le vérificateur et effectuées dans l'anneau des entiers modulo N,

- le vérifié délivre au vérificateur un nombre t, appelé témoin, résultat de ces opérations,

- le vérificateur effectue à son tour des opérations portant sur le témoin t délivré par le vérifié et sur l'identité ombragée J du vérifié, opérations liées elles aussi au nombre D tiré au hasard par le vérificateur et effectuées dans l'anneau des entiers modulo N,

- le vérificateur compare le résultat ainsi obtenu avec les bits du titre T que le vérifié a délivré en début de processus de vérification, et admet l'authenticité de l'accréditation s'il retrouve ces bits.

Le procédé d'authentification d'accréditation selon l'invention est caractérisé par le fait que :

a) lors de l'élaboration de l'accréditation (B) le nombre p servant à extraire la racine p ième de l'identité ombragée (J) est choisi grand et comprend au moins une dizaine de bits,

b) pour l'authentification de l'accréditation le processus ne comprend qu'un seul traitement interactif et probabiliste (et non une répétition d'un tel traitement), ce traitement unique consistant dans les opérations suivantes :

- le nombre que le vérificateur tire au hasard est un entier D compris entre 0 et p-1 (bornes incluses),

- l'opération que le vérifié effectue pour délivrer un témoin t est le produit, dans l'anneau des entiers modulo N, de l'élément r qu'il a lui même tiré au hasard, par la puissance Dième de l'accréditation inverse B, le titre étant alors $t=r.B^{D} \bmod N$,

- les opérations qu'effectue le vérificateur sont le

produit, dans l'anneau des entiers modulo N, de la puissance p ième du témoin t par la puissance D ième de l'identité ombragée J, soit $t^p J^D \bmod N$,

- l'opération de comparaison effectuée par le vérificateur porte alors sur les bits du titre T délivrés par le vérifié et sur les bits obtenus par l'opération précédente, l'authenticité de l'accréditation étant acquise en un seul traitement dès lors que tous les bits du titre délivré par le vérifié sont retrouvés par le vérificateur dans $t^p J^D \bmod N$.

Pour ce qui est du procédé d'authentification de message, le procédé selon l'invention est caractérisé par le fait que :

a) lors de l'élaboration de l'accréditation du donneur d'ordre, le nombre p servant à extraire la racine p ième de l'identité ombragée est choisi grand et comprend au moins une dizaine de bits,

b) pour l'authentification du message, le processus ne comprend qu'un seul traitement interactif et probabiliste (et non une répétition d'un tel traitement), ce traitement unique consistant dans les opérations suivantes :

- le nombre que le vérificateur tire au hasard est un entier D compris entre 0 et p-1 (bornes incluses),

- l'opération que le vérifié effectue pour délivrer le témoin t est le produit, dans l'anneau des entiers modulo N, de l'élément r qu'il a lui même tiré, par la puissance Dième de l'accréditation inverse B, le témoin étant alors $r.B^D \bmod N$,

- les opérations qu'effectue le vérificateur sont le produit, dans l'anneau des entiers modulo N, de la puissance p ième du témoin t, par la puissance D ième de l'identité ombragée J,

- le vérificateur forme la fonction de compression du message et du résultat des opérations précédentes soit $f(m, t^p J^D \bmod N)$,

- la comparaison que le vérificateur effectue porte

alors sur la fonction de compression qu'il a obtenue et sur le titre T que le vérifié lui a délivré en début de processus de vérification, l'authenticité du message étant acquise en un seul traitement dès lors que, à la fin de ce traitement, il y a correspondance entre tous les bits de la fonction de compression obtenue par le vérificateur et les bits du titre délivrés par le vérifié.

L'invention a enfin pour objet un procédé de signature de message. Dans ce cas l'accréditation du signataire est élaborée selon le procédé connu à clé publique décrit plus haut et la signature consiste en un traitement numérique probabiliste connu comprenant les opérations suivantes :

- le signataire tire au hasards au moins un entier r appartenant à l'anneau des entiers modulo N,
- le signataire élève cet entier r à la puissance p modulo N,
- le signataire calcule une fonction de compression f en prenant comme arguments le message m à signer et la puissance $r^D$ mod N obtenue,
- le signataire forme au moins un témoin t en effectuant certaines opérations sur r et sur l'accréditation inverse B, ces opérations étant liées au nombre D tiré au hasard et étant effectuées dans l'anneau des entiers modulo N,
- le signataire transmet le message m, son identité I, le mot D, le ou les témoins t, l'ensemble constituant un message signé.

Le procédé de signature de message selon l'invention est caractérisé par le fait que :

a) lors de l'élaboration de l'accréditation du signataire le nombre p servant à extraire la racine p ième de l'identité ombragée est choisi grand et comprend plusieurs dizaines de bits,

b) pour l'opération de signature du message :

- le signataire ne tire au hasard qu'un seul entier r appartenant à l'anneau des entiers modulo N,

- la fonction de compression a pour arguments le message m et la puissance p ième de r, ce qui fournit un nombre D,

- le titre unique produit par le signataire est le produit, dans l'anneau des entiers modulo N, de l'entier r par la puissance D ième de l'accréditation inverse B,

- le signataire fournit, avec le message m, son identité I, le mot D et le titre t.

Dans les deux premiers procédés, le nombre p comprend au moins 10 bits et de préférence entre 16 et 24 bits.

Dans le procédé de signature le nombre p est plus grand et comprend plusieurs dizaines de bits, par exemple de 60 à 80 bits.

La valeur de p est en effet le facteur de sécurité d'un traitement élémentaire. Si p est convenable pour le but recherché alors qu'on ne dispose que d'une seule accréditation profonde, on peut se contenter d'un seul traitement.

De toute façon l'invention sera mieux comprise à la lumière de la description qui va suivre, qui se réfère à des dessins annexés. Ces dessins comprennent :

- les figures 1 à 6, déjà décrites, qui illustrent les procédés S et FS de l'art antérieur ;

- la figure 7 illustre le procédé d'authentification d'une accréditation selon l'invention ;

- la figure 8 illustre le procédé d'authentification de message selon l'invention ;

- la figure 9 illustre le procédé de signature de message selon l'invention ;

- la figure 10 montre schématiquement un ensemble permettant de mettre en oeuvre les procédés de l'invention.

Les conventions utilisées dans les figures 7 à 9 sont les mêmes que celles des figures 1 à 6. Dans tous les cas l'accréditation est obtenue par l'utilisation d'un nombre p qui est grand. Les inventeurs qualifient cette accréditation de "profonde" par opposition aux accréditations habituelles

utilisées dans ce domaine pour lesquelles p était de l'ordre de 2 ou 3 et qui sont, en quelque sorte "superficielles".

Dans le cas des cartes à puce on a donc, dans le cas de l'invention, le traitement suivant :

- la carte tire au hasard un élément r ($1 \leq r \leq N-1$) dans l'anneau des entiers modulo N, et donne en guise de titre T 128 bits de la puissance publique de cet élément ($r^p \bmod N$) ;
- le vérificateur tire au hasard un exposant D de 0 à p-1 et le transmet à la carte ;
- la carte calcule le témoin t qui est le produit (dans l'anneau) de l'élément r par la puissance D ième de l'accréditation B ($t=r.B^D \bmod N$) ;
- le vérificateur calcule dans l'anneau le produit de la puissance p ième du témoin t par la puissance D ième de l'identité ombragée J, soit $t^p.J^D \bmod N$.

La preuve est acceptée si tous les bits publiés du titre T sont ainsi retrouvés.

N'importe qui ayant deviné la question du vérificateur (lexposant D) peut tirer au hasard un témoin t, puis faire à l'avance les calculs du vérificateur, c'est-à-dire faire le produit dans l'anneau du témoin t à l'exposant p par l'identité ombragée J à l'exposant D. En donnant le titre T au début de l'itération, si la question posée est bien D, alors le témoin t est une réponse acceptable.

Ce raisonnement indiquant une stratégie gagnante pour le devin montre que l'on ne sait pas distinguer des données provenant de l'enregistrement d'une transaction réussie et des données provenant d'une mascarade construite en inversant la chronologie de l'itération, c'est-à-dire en choisissant les exposants avant les titres. Le vérificateur recueille des informations impossibles à distinguer de celles qu'il aurait pu produire tout seul, sans interaction avec le vérifié, ce qui montre que l'accréditation reste bien secrète dans la carte.

Pour passer avec succès un traitement d'authentification, le bluffeur doit deviner un exposant D. Si

les p valeurs de D sont équiprobables, la chance laissée au bluffeur est de 1/p. Le facteur de sécurité est donc p.

Dans un tel traitement le vérifié transmet une centaine de bits et un élément de l'anneau ; le vérificateur transmet un exposant (D). Pour mener à bien un traitement le vérifié calcule d'abord la puissance publique de l'élément r tiré au hasard, puis le produit de cet élément r par la puissance D ième de l'accréditation B. Le vérificateur fait un peu moins de calcul pour retrouver le titre T car il peut combiner intelligemment les calculs de puissance : la puissance Dième de l'identité ombragée J et la puissance pième du témoin t.

Si l'exposant p vaut $2^{16}$, alors l'exposant D est un nombre de 16 bits. Ainsi en un seul traitement, avec un facteur de sécurité de $2^{16}$, soit 65536, le vérifié calcule dans l'anneau 16 carrés, puis 16 carrés et une moyenne de 8 multiplications. Le vérificateur ne calcule que 16 carrés et procède en moyenne à 8 multiplications.

Le procédé d'authentification de message est illustré sur la figure 8 avec les mêmes conventions, la différence avec la figure 7 consistant uniquement dans la formation de la fonction de compression f.

Pour signer un message, le détenteur de l'accréditation B de profondeur p commence par tirer au hasard un élément r dans l'anneau puis calcule la puissance publique de l'élément $r(r^p \bmod N)$. Puis il produit un exposant D grâce à la fonction de compression f appliquée à la concaténation du message m et de la puissance publique de l'élément r. Le témoin t est le produit de l'élément r par la puissance Dième de l'accréditation B. Le message signé est la concaténation de l'identité I, du message m, de l'exposant d et du témoin t.

Pour vérifier une signature, le vérificateur calcule dans l'anneau le produit du témoin t à la puissance p par l'identité ombragée J (reconstruite à partir de l'identité proclamée I) à la puissance D pour reconstituer ce qui doit être la puissance publique de l'élément r. Enfin, le vérificateur doit

retrouver l'exposant D en appliquant la fonction f à la concaténation du message m et de la puissance publique reconstituée.

C'est ce qui est illustré sur la figure 9.

Si p s'écrit sur 64 bits quelconques, le signataire fait environ 192 multiplications dans l'anneau (il doit calculer successivement deux puissances avec des exposants de 64 bits sans pouvoir les combiner) pour mener à bien l'opération. Cette complexité est déjà nettement inférieure à celle du procédé RSA : 768 multiplications en moyenne pour une exponentielle modulo un nombre composé sur 512 bits, et 1536 pour un nombre composé sur 1024 bits.

Si p s'écrit sur 64 bits quelconques, le vérificateur fait seulement environ 112 multiplications, car il combine ses opérations en 64 carrés et trois fois 16 multiplications en moyenne, pour calculer d'un seul coup $t^p.J^D \bmod N$. Il est heureux que l'authentification soit plus simple que l'élaboration de la signature, car chaque signature est appelée à être vérifiée plusieurs fois.

Mais, on peut choisir $2^{64}$ (c'est-à-dire une puissance de 2) comme exposant p pour simplifier les calculs, sans modifier la sécurité du système. L'élévation à la puissance p se fait alors par 64 carrés. L'exposant D est un nombre de 64 bits. La signature se fait alors en 160 multiplications. La vérification d'une signature se traduit en moyenne par 96 multiplications dans l'anneau, soit 12,5% du RSA à 512 bits et 6,2% du RSA à 1024 bits.

Dans le procédé antérieur FS décrit plus haut, avec 64 accréditations multiples dans la même carte, il faut un carré et une moyenne de 32 multiplications. Ainsi, la méthode de l'invention à accréditation profonde, se paye par un surplus de calculs d'un facteur multiplicatif de l'ordre de 3. Quand, dans l'art antérieur, on se limite à 8 accréditations dans la carte, avec 8 témoins dans la signature, (8 itérations à 5 multiplications, soit 40 multiplications), le rapport diminue

encore un peu, en faveur de l'invention.

Bien entendu, on peut aussi choisir $2^{64}+1$ comme exposant public (c'est-à-dire un nombre impair). Au prix d'une seule multiplication supplémentaire pour calculer une puissance publique, on lève ainsi certaines restrictions relatives aux résidus quadratiques dans l'anneau (lorsque l'exposant p est pair, plusieurs éléments de l'anneau pouvant correspondre à la racine pième, mais un seul convenant).

La figure 10 représente schématiquement un calculateur permettant de mettre en oeuvre l'invention.

Le calculateur représenté comprend une interface entrées-sorties ES, une unité centrale UC, une mémoire programmable du type à lecture seulement (PROM), une mémoire à lecture seulement (ROM) et une mémoire à accès direct (RAM). Le calculateur comprend encore un organe G du type générateur de bruit ou générateur aléatoire.

L'accréditation et les informations d'identité inscrites dans la mémoire PROM sont inaccessibles de l'extérieur. Les programmes sont inscrits dans la mémoire ROM. La mémoire RAM sert à stocker des résultats de calcul. Le générateur G est utilisé pour les tirages au sort des divers nombres intervenant dans le procédé (r, D).

L'unité centrale et les mémoires peuvent être structurées comme le microcalculateur autoprogrammable monolithique décrit dans le brevet 4,382,279 des Etats-Unis d'Amérique.

La fonction de compression peut faire appel à l'algorithme DES (Data Encryption Standard). Il existe une carte à puce, fabriquée par PHILIPS qui réalise cet algorithme DES.

REVENDICATIONS

1. Procédé d'authentification d'une accréditation à apport nul de connaissance,

a) cette accréditation ayant été élaborée par un procédé du type à clé publique comprenant les opérations suivantes :

- une autorité habilitée à délivrer des accréditations choisit deux nombres premiers, forme le produit (N) de ces deux nombres, tient secrets ces nombres, choisit un entier p et publie N et p;

- pour chaque détenteur d'une accréditation, une identité numérique I est constituée, puis complétée par redondance pour former un mot J appelé identité ombragée,

- une accréditation A est élaborée par l'autorité en prenant la racine pième de l'identité ombragée dans l'anneau des entiers modulo N ($A = J^{1/p} \bmod N$),

- dans un support approprié contenant une mémoire, l'autorité charge l'inverse modulo N de l'accréditation A soit un nombre B appelé accréditation inverse ($B^n J \bmod N=1$), ce nombre B constituant l'accréditation qu'il s'agit d'authentifier,

b) l'authentification de l'accréditation ainsi élaborée, consistant en un processus numérique interactif et probabiliste du type à apport nul de connaissance et s'établissant entre un support contenant une accréditation, support appelé "le vérifié" et un organe d'authentification appelé "le vérificateur", ce processus comprenant au moins un traitement numérique constitué par les opérations connues suivantes :

- le vérifié tire d'abord au hasard un entier r appartenant à l'anneau des entiers modulo N,

- le vérifié élève cet entier r à la puissance p modulo N, le résultat étant appelé titre T,

- le vérifié délivre alors au moins une partie des bits du titre T,

- le vérificateur tire ensuite au hasard un nombre (d) et demande au vérifié d'effectuer certaines opérations sur r et sur l'accréditation inverse B, ces opérations étant liées au nombre (d) tiré au hasard par le vérificateur et effectuées dans l'anneau des entiers modulo N,

- le vérifié délivre au vérificateur un nombre t, appelé témoin, résultat de ces opérations,

- le vérificateur effectue à son tour des opérations portant sur le témoin t délivré par le vérifié et sur l'identité ombragée J du vérifié, opérations liées elles aussi au nombre d tiré au hasard par le vérificateur et effectuées dans l'anneau des entiers modulo N,

- le vérificateur compare le résultat ainsi obtenu avec les bits du titre T que le vérifié a délivré en début de processus de vérification, et admet l'authenticité de l'accréditation s'il retrouve ces bits,

ce procédé étant caractérisé par le fait que :

a) lors de l'élaboration de l'accréditation (B) le nombre p servant à extraire la racine p ième de l'identité ombragée (J) est choisi grand et comprend au moins une dizaine de bits,

b) pour l'authentification de l'accréditation le processus ne comprend qu'un seul traitement interactif et probabiliste (et non une répétition d'un tel traitement), ce traitement unique consistant dans les opérations suivantes :

- le nombre que le vérificateur tire au hasard est un entier D compris entre 0 et p-1 (bornes incluses),

- l'opération que le vérifié effectue pour délivrer un témoin t est le produit, dans l'anneau des entiers modulo N, de l'élément r qu'il a lui même tiré au hasard, par la puissance Dième de l'accréditation inverse B, le titre étant alors $t=r.B^{D} \bmod N$,

- les opérations qu'effectue le vérificateur sont le produit, dans l'anneau des entiers modulo N, de la puissance p ième du témoin t par la puissance D ième de l'identité ombragée J, soit $t^{p} J^{D} \bmod N$,

- l'opération de comparaison effectuée par le vérificateur porte alors sur les bits du titre T délivrés par le vérifié et sur les bits obtenus par l'opération précédente, l'authenticité de l'accréditation étant acquise en un seul traitement dès lors que tous les bits du titre délivré par le vérifié sont retrouvés par le vérificateur dans $t^p J^D \bmod N$.

2. Procédé d'authentification d'un message, ce message provenant d'un donneur d'ordre censé être accrédité :

a) l'accréditation d'un donneur d'ordre consistant en un mot numérique B obtenu par un procédé à clé publique comprenant les opérations suivantes :

- une autorité habilitée à délivrer des accréditations choisit deux nombre premiers, forme le produit N de ces deux nombres, tient secrets ces deux nombres, choisit un entier p et publie N et p,

- pour chaque donneur d'ordre une identité numérique I est constituée puis complétée par redondance pour former un mot J appelé identité ombragée,

- une accréditation A est élaborée par l'autorité en prenant la racine p ième de l'identité ombragée J dans l'anneau des entiers modulo N, ($A = J^{1/p} \bmod N$),

- dans un support approprié détenu par le donneur d'ordre l'autorité charge l'inverse modulo N de l'accréditation A, soit un nombre B appelé accréditation inverse ($B^p J \bmod N=1$),

b) l'authentification d'un message (m) émis par un donneur d'ordre ainsi accrédité consistant en un processus numérique interactif et probabiliste du type à apport nul de connaissance et s'établissant entre le support du donneur d'ordre censé accrédité et appelé "le vérifié" et un organe de vérification appelé "le vérificateur", ce processus comprenant au moins un traitement numérique constitué par les opérations suivantes :

- le vérifié tire d'abord au hasard un entier r appartenant à l'anneau des entiers modulo N,

- le vérifié élève cet entier r à la puissance p modulo N et calcule un résultat par une fonction de compression en prenant comme argument le message m et $r^p$ mod N, soit f(m, $r^p$ mod N), le résultat étant appelé titre T,

- le vérifié délivre alors au moins une partie des bits de titre T,

- le vérificateur tire ensuite au hasard un nombre d et demande au vérifié d'effectuer certaines opérations sur r et sur l'accréditation inverse B, ces opérations étant liées au nombre d tiré au hasard par le vérificateur et étant effectuées dans l'anneau des entiers modulo N,

- le vérifié fournit au vérificateur un nombre t, appelé témoin, résultat de ces opérations,

- le vérificateur effectue à son tour des opérations portant sur le témoin t délivré par le vérifié et sur l'identité ombragée J du vérifié, opérations liées elles aussi au nombre D tiré au hasard par le vérificateur et effectuées dans l'anneau des entiers modulo N,

- le vérificateur forme une fonction de compression en prenant comme arguments le message à authentifier m et le résultat des opérations précédentes, soit f(m, t, J),

- le vérificateur compare la fonction de compression obtenue avec le titre T que le vérifié a délivré en début de processus de vérification,

ce processus étant caractérisé par le fait que :

a) lors de l'élaboration de l'accréditation du donneur d'ordre, le nombre p servant à extraire la racine p ième de l'identité ombragée est choisi grand et comprend au moins une dizaine de bits,

b) pour l'authentification du message, le processus ne comprend qu'un seul traitement interactif et probabiliste (et non une répétition d'un tel traitement), ce traitement unique consistant dans les opérations suivantes :

- le nombre que le vérificateur tire au hasard est un entier D compris entre 0 et p-1 (bornes incluses),

- l'opération que le vérifié effectue pour délivrer le témoin t est le produit, dans l'anneau des entiers modulo N, de l'élément r qu'il a lui même tiré, par la puissance Dième de l'accréditation inverse B, le témoin étant alors $r.B^D \bmod N$,

- les opérations qu'effectue le vérificateur sont le produit, dans l'anneau des entiers modulo N, de la puissance p ième du témoin t, par la puissance D ième de l'identité ombragée J,

- le vérificateur forme la fonction de compression du message et du résultat des opérations précédentes soit $f(m, t^p J^D \bmod N)$,

- la comparaison que le vérificateur effectue porte alors sur la fonction de compression qu'il a obtenue et sur le titre T que le vérifié lui a délivré en début de processus de vérification, l'authenticité du message étant acquise en un seul traitement dès lors que, à la fin de ce traitement, il y a correspondance entre tous les bits de la fonction de compression obtenue par le vérificateur et les bits du titre délivrés par le vérifié.

3. Procédé de signature d'un message par une entité, cette entité étant censée être accréditée,

a) l'accréditation d'une entité signataire de messages ayant été élaborée par un procédé à clé publique comprenant les opérations suivantes :

- une autorité habilitée à délivrer des accréditations choisit deux nombres premiers, forme le produit N de ces deux nombres, tient secrets les deux nombres premiers, choisit un entier p et publie N et p,

- pour chaque entité signataire une identité numérique I est constituée puis complétée par redondance pour former un mot J appelé identité ombragée,

- une accréditation A est élaborée par l'autorité en prenant la racine p ième de l'identité ombragée J dans l'anneau des entiers modulo N ($A = J^{1/p} \bmod N$),

- dans un support approprié détenu par le signataire l'autorité charge l'inverse modulo N de l'accréditation A, soit un nombre B appelé accréditation inverse ($B^p$ J mod N=1),

b) la signature d'un message m par un signataire d'identité I consistant en un traitement numérique probabiliste comprenant les opérations suivantes :

- le signataire tire au hasard au moins un entier r appartenant à l'anneau des entiers modulo N,
- le signataire élève cet entier r à la puissance p modulo N,
- le signataire calcule une fonction de compression f en prenant comme arguments le message m à signer et la puissance $r^p$ obtenue,
- le signataire forme au moins un témoin t en effectuant certaines opérations sur r et sur l'accréditation inverse B, ces opérations étant liées au nombre d tire au hasard et étant effectuées dans l'anneau des entiers modulo N,
- le signataire transmet le message m, son identité I, le mot d, le ou les témoins t, l'ensemble constituant un message signé,

ce procédé étant caractérisé par le fait que :

a) lors de l'élaboraton de l'accréditation du signataire le nombre p servant à extraire la racine p ième de l'identité ombragée est choisi grand et comprend plusieurs dizaines de bits,

b) pour l'opération de signature du message :

- le signataire ne tire au hasard qu'un seul entier r appartenant à l'anneau des entiers modulo N,
- la fonction de compression a pour arguments le message m et la puissance p ième de r, ce qui fournit un nombre D,
- le témoin unique produit par le signataire est le produit, dans l'anneau des entiers modulo N, de l'entier r par la puissance D ième de l'accréditation inverse B,
- le signataire fournit, avec le message m, son identité I, le mot D et le témoin t.

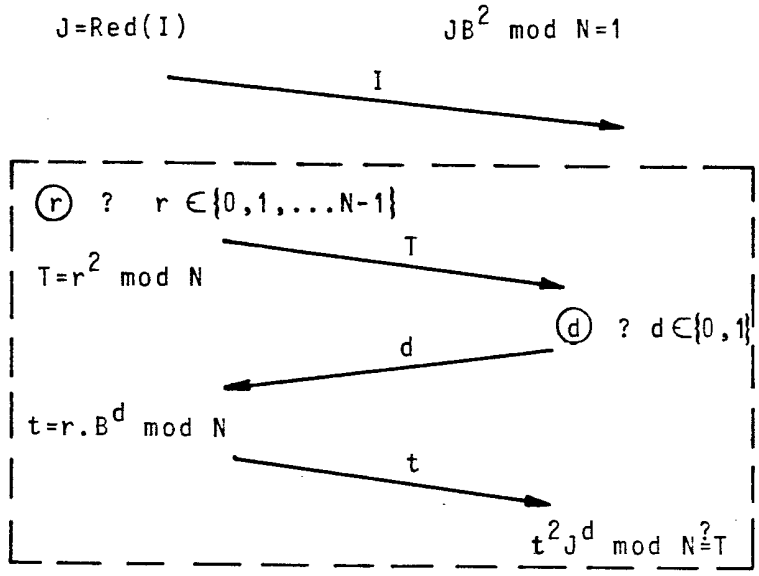

J=Red(I)
JB² mod N=1
I
r ? r ∈{0,1,...N-1}
T
T=r² mod N
d ? d∈{0,1}
d
t=r.B^d mod N
t
t²J^d mod N≟T

FIG. 1

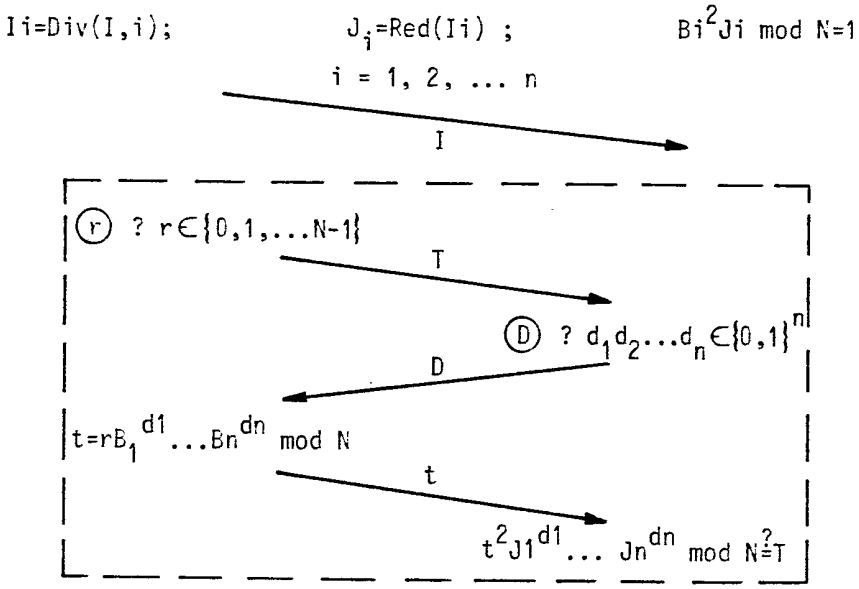

Ii=Div(I,i);
J_i=Red(Ii) ;
Bi²Ji mod N=1
i = 1, 2, ... n
I
r ? r∈{0,1,...N-1}
T
D ? d1d2...dn∈{0,1}^n
D
t=rB1^d1...Bn^dn mod N
t
t²J1^d1... Jn^dn mod N≟T

FIG. 2

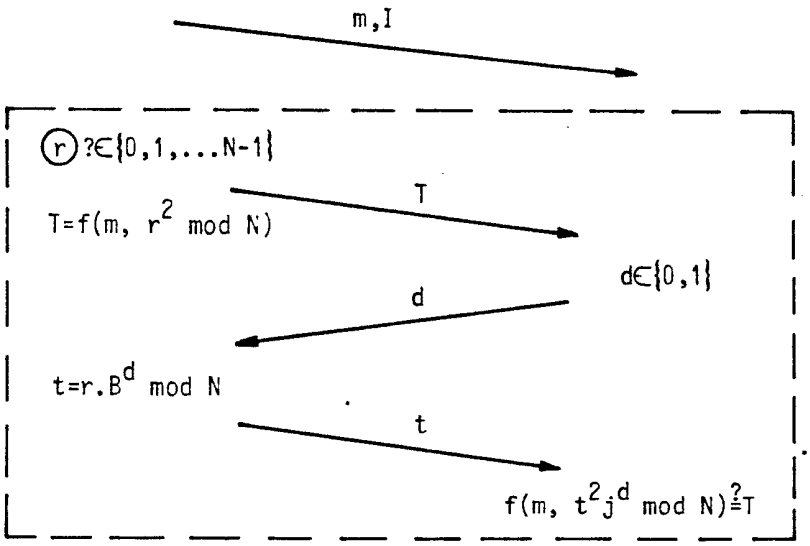

m,I
r ?∈{0,1,...N-1}
T=f(m, r^2 mod N)
T
d∈{0,1}
d
t=r.B^d mod N
t
f(m, t^2 j^d mod N) ≟ T

FIG. 3

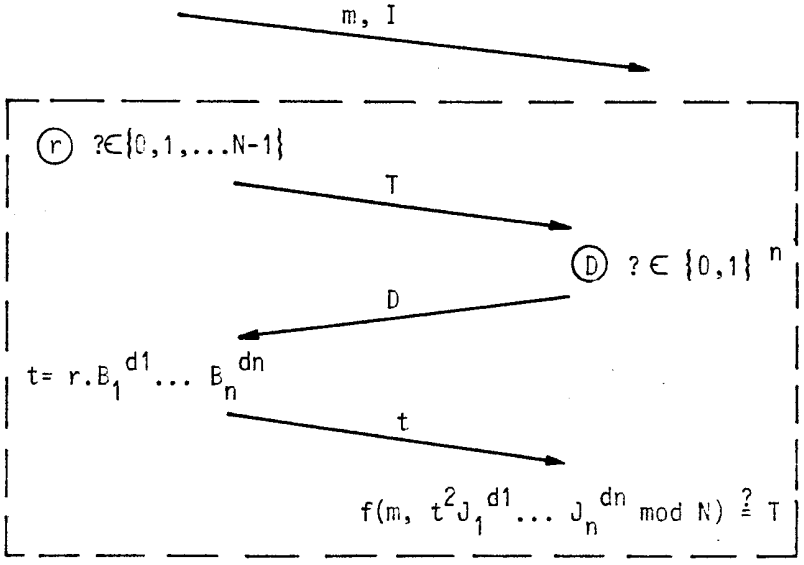

m, I
r ?∈{0,1,...N-1}
T
D ? ∈ {0,1}^n
D
t= r.B_1^d1 ... B_n^dn
t
f(m, t^2 J_1^d1 ... J_n^dn mod N) ≟ T

FIG. 4

FIG. 5

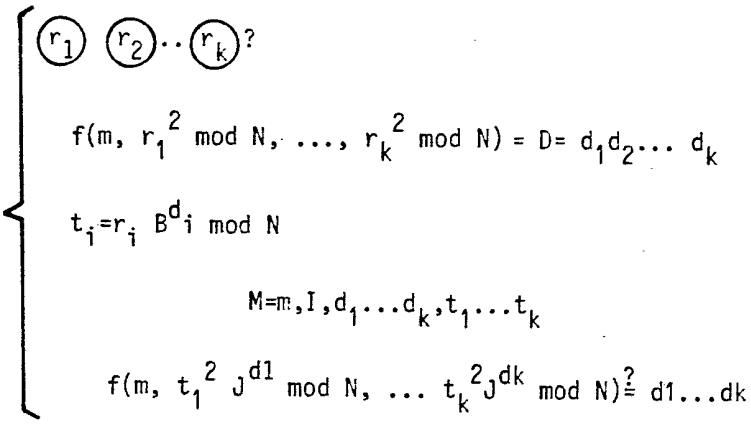
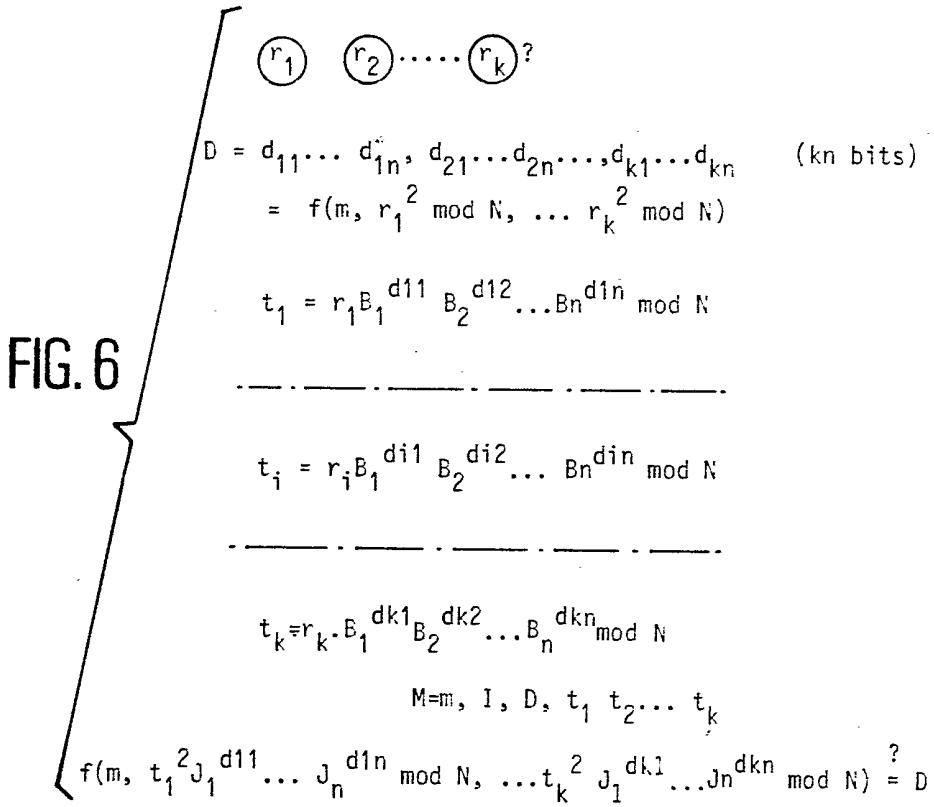

(r1) (r2).. (rk)?
f(m, r1^2 mod N, ..., rk^2 mod N) = D= d1d2... dk
ti=ri B^di mod N
M=m,I,d1...dk,t1...tk
f(m, t1^2 J^d1 mod N, ... tk^2 J^dk mod N)? d1...dk

FIG. 6


(r1) (r2)..... (rk)?
D = d11... d1n, d21...d2n...,dk1...dkn (kn bits)
= f(m, r1^2 mod N, ... rk^2 mod N)
t1 = r1B1^d11 B2^d12...Bn^d1n mod N
ti = riB1^di1 B2^di2... Bn^din mod N
tk=rk.B1^dk1B2^dk2...Bn^dkn mod N
M=m, I, D, t1 t2... tk
f(m, t1^2J1^d11... Jn^d1n mod N, ...tk^2 J1^dk1...Jn^dkn mod N) ? D

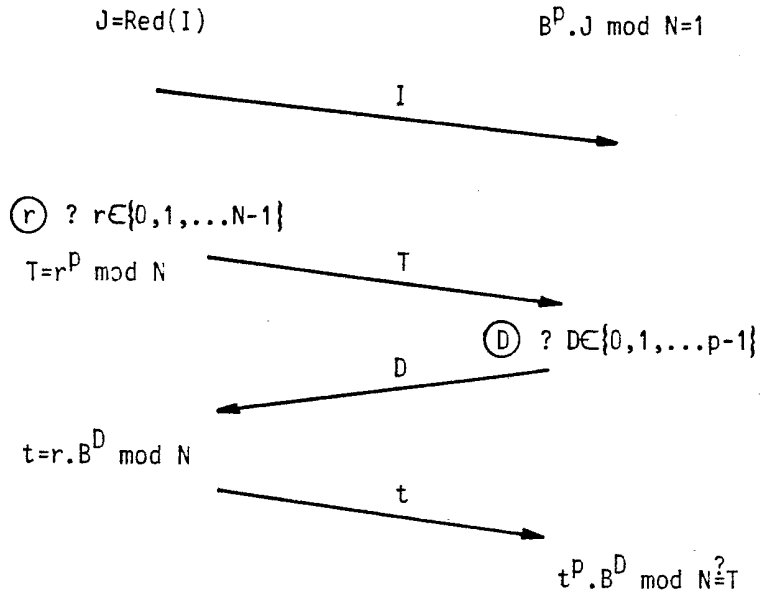

J=Red(I)
$B^P.J \bmod N=1$
I
(r) ? r∈{0,1,...N-1}
$T=r^P \bmod N$
T
(D) ? D∈{0,1,...p-1}
D
$t=r.B^D \bmod N$
t
$t^P.B^D \bmod N \stackrel{?}{=} T$

FIG. 7

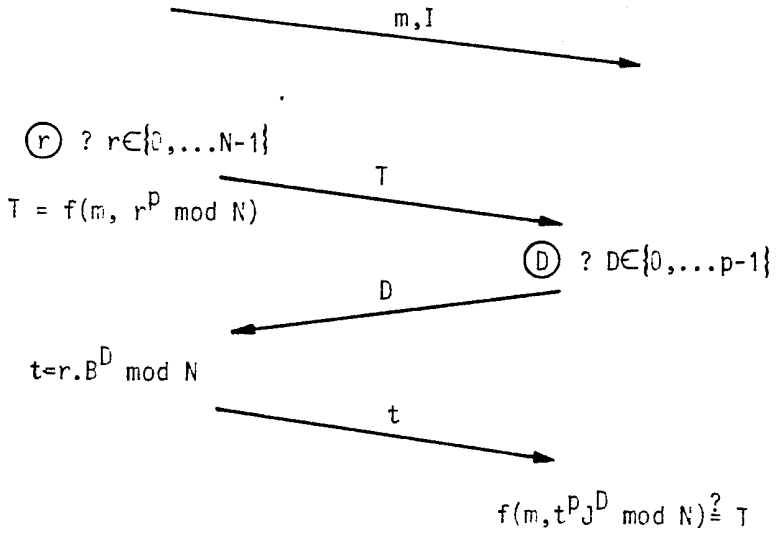
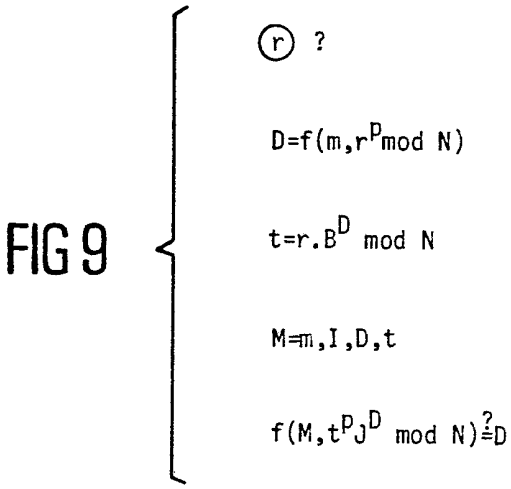

m,I
(r) ? r∈{0,...N-1}
$T = f(m, r^P \bmod N)$
T
(D) ? D∈{0,...p-1}
D
$t=r.B^D \bmod N$
t
$f(m,t^P J^D \bmod N) \stackrel{?}{=} T$

FIG. 8

FIG 9



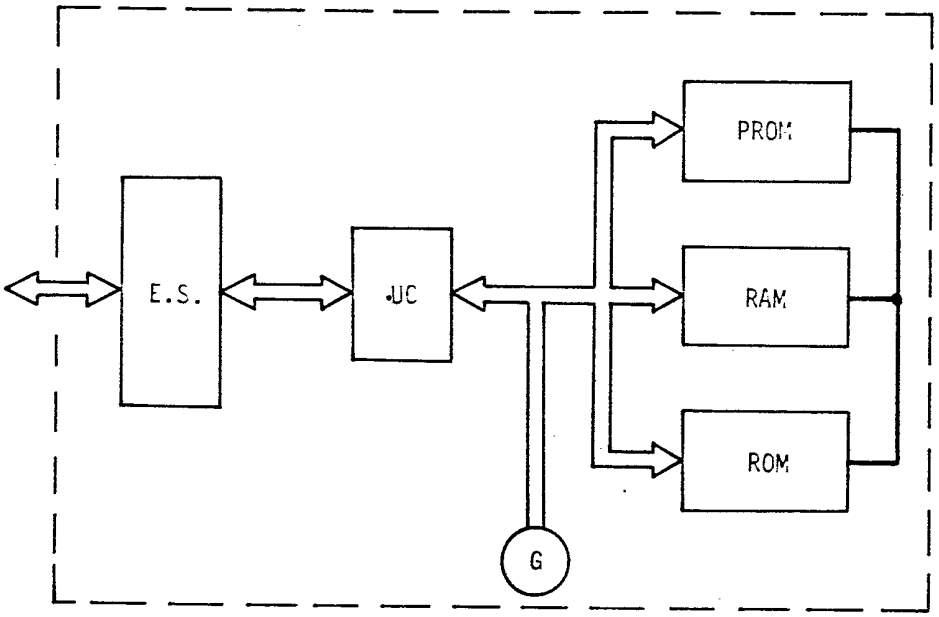




FIG. 10