(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 714 780**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **93 15879**

(51) Int Cl⁶ : H 04 L 9/32, 9/30, G 06 F 7/58//G 07 F 7/10

# (12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 30.12.93.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 07.07.95 Bulletin 95/27.

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

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

(71) **Demandeur(s) :** *STERN Jacques* — FR.

(72) **Inventeur(s) :** STERN Jacques.

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

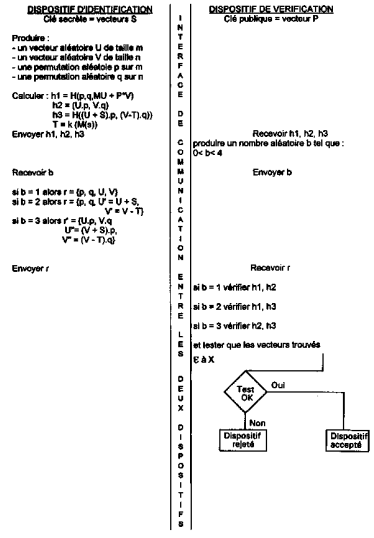
(74) **Mandataire :** Thomson Consumer Electronics.

## (54) Procédé d'authentification d'au moins un dispositif d'identification par un dispositif de vérification.

(57) La présente invention concerne un nouveau procédé d'authentification d'au moins un dispositif d'identification par un dispositif de vérification. Ce procédé est basé sur des techniques cryptographiques à clés secrètes et publiques, l'authentification étant réalisée par un protocole à apport nul de connaissance.

De plus, ce dialogue est établi en utilisant le problèmes des équations linéaires contraintes.

L'invention s'applique à la cryptologie.




FR 2 714 780 - A1

# PROCEDE D'AUTHENTIFICATION D'AU MOINS UN DISPOSITIF D'IDENTIFICATION PAR UN DISPOSITIF DE VERIFICATION

La présente invention concerne un nouveau procédé d'authentification d'au moins un dispositif d'identification par un dispositif de vérification, cette authentification étant réalisée par un protocole à apport nul de connaissance basé sur le problème des équations linéaires contraintes.

Le problème des équations linéaires contraintes (Constrained linear equations : CLE en langue anglaise) consiste à trouver des valeurs satisfaisant un certain nombre d'équations linéaires modulo un nombre premier d, ces valeurs étant de plus contraintes à se trouver dans un ensemble prescrit X.

La présente invention s'applique plus particulièrement au cas des communications dites sécurisées où deux dispositifs échangent des données à travers un canal dont la sécurité est suspecte. Dans ce cas, il est essentiel d'avoir un moyen de reconnaissance mutuelle, à savoir un moyen permettant au dispositif de vérification d'authentifier un utilisateur et de lui permettre un accès aux données ou au service. Il existe de nombreux exemples nécessitant la mise en oeuvre de ce type de communication sécurisée. On peut citer, notamment, le cas des ordinateurs de type bancaire permettant d'effectuer des transferts d'ordre, des distributeurs automatiques de billets, des décodeurs de télévision à péage, des publiphones.

Dans ce contexte, on utilise fréquemment des méthodes d'authentification qui sont basées sur des techniques cryptographiques à clés secrètes. Ces méthodes sont, jusqu'à ce jour, les plus simples à mettre en oeuvre. Dans le cadre de ces méthodes, le dispositif d'identification, en général une carte à puce, et le dispositif de vérification tel qu'un lecteur de carte, un décodeur, un publiphone, partagent la même clé secrète et l'identification est accomplie par un algorithme symétrique ou une fonction à sens unique.

L'inconvénient de ces méthodes réside dans le fait que les deux parties, à savoir le dispositif de vérification et le dispositif d'identification, doivent coopérer mutuellement et secrètement. Cette condition n'est pas toujours vérifiée. En effet, un élément pirate peut acheter le dispositif de vérification et l'analyser pour connaître sa

structure interne. Ensuite, l'élément pirate est techniquement capable de réaliser des dispositifs d'identification performants, car les clés secrètes sont présentes aux deux extrémités du réseau, à savoir dans le dispositif de vérification et dans le dispositif d'identification.

Il est reconnu que, parmi les divers procédés pouvant être implémentés pour se prémunir contre les inconvénients des méthodes classiques connues, les protocoles à apport nul de connaissance assurent jusqu'à maintenant le degré de sécurité le plus élevé. Ces protocoles à apport nul de connaissance sont fonctionnellement caractérisés par le fait qu'un nombre illimité d'interactions avec le dispositif d'identification et une analyse complète de la structure du dispositif de vérification ne sont pas suffisants pour pouvoir reconstruire les dispositifs d'identification. On peut trouver une description des procédés d'identification à apport nul de connaissance existant notamment dans le brevet américain N° 4 748 668 au nom de FIAT et al. ou dans le brevet américain US-A-4 932 056 au nom de Shamir. Ce dernier brevet décrit une méthode d'authentification basée sur le problème des noyaux permutés, cette méthode étant connue sous le nom de méthode PKP.

Le présent inventeur a aussi mis au point un nouveau procédé d'authentification basé sur le problème du décodage par syndrome. Cette méthode est décrite dans l'article intitulé "A new identification scheme based on syndrome decoding" de Jacques STERN présenté au congrès CRYPTO 93 (Actes à paraître dans la collection "Lecture Notes in Computer Science"). L'inconvénient des différentes méthodes décrites ci-dessus est d'être relativement lentes lors des échanges entre les dispositifs de vérification et d'identification. D'autre part, les clés publiques ou secrètes utilisées dans ces méthodes sont en général codées sur un nombre de bits très important, nécessitant une puissance de calcul élevée et une place mémoire non négligeable.

La présente invention a donc pour but de remédier aux inconvénients mentionnés ci-dessus en proposant un nouveau procédé d'authentification qui permet une authentification rapide du dispositif d'identification par le dispositif de vérification et autorise l'emploi de clés , tant publiques que secrètes, de taille modérée.

La présente invention a pour objet un procédé d'authentification d'au moins un dispositif de vérification basé sur des

techniques cryptographiques à clés secrètes et publiques, l'authentification étant réalisée par un protocole à apport nul de connaissance, caractérisé en ce que la clé publique est établie en utilisant les équations linéaires contraintes. De préférence, ce procédé est caractérisé par les étapes suivantes :

- pour permettre le dialogue entre le dispositif d'identification et le dispositif de vérification, établir une clé secrète constituée par au moins un vecteur S de dimension n dont les coordonnées sont choisies dans un ensemble X fixé et une clé publique comprenant une matrice M de dimensions m x n dont les coefficients sont choisis aléatoirement parmi les entiers compris entre 0 et d-1 où d est un nombre premier proche du carré d'un nombre c, et au moins un vecteur P tel que $P = g(M(S))$ où g désigne une fonction qui est définie à partir de l'ensemble X et d'un sous groupe G de l'ensemble des entiers (1, 2, ...d-1) et qui associe à chaque coordonnée x du vecteur, un élément g(x) de G tel que x s'écrive d'une manière unique comme produit de g(x) et d'un élément k(x) de X,

- au niveau du dispositif d'identification, recevoir un ou plusieurs éléments aléatoires produits par le dispositif de vérification et envoyer au dispositif de vérification un engagement obtenu en appliquant une fonction de hachage cryptographique sur des paramètres fonctions de S, de M et des éléments aléatoires ,

- puis, en fonction du ou des nombres aléatoires tirés par le dispositif de vérification, tester au niveau du dispositif de vérification à l'aide des éléments reçus et de la clé publique, que les engagements sont corrects,

- répéter les opérations précédentes un nombre de fois fonction du niveau de sécurité souhaité.

Dans le procédé d'authentification ci-dessus, on utilise une matrice M de dimensions m x n, cette matrice étant commune à tous les utilisateurs et construite aléatoirement. Chaque utilisateur reçoit une clé secrète S qui est un mot de n bits dont les coordonnées sont choisies dans un ensemble X fixé. L'ensemble X est formé de c éléments, tels que tout entier compris entre 1 et d-1 s'écrive de manière unique comme produit d'un élément de G et d'un élément de X. Dans ce cas, le système calcule la clé publique P telle que $P = g(M(S))$.

D'autre part, le procédé d'identification est basé principalement sur la notion technique d'engagement. Si U est une séquence d'éléments binaires, un engagement pour U est l'image de U à travers une certaine fonction de hachage cryptographique. L'engagement sera utilisé comme une fonction à sens unique. La fonction de hachage proprement dite peut être réalisée par exemple suivant la méthode présentée par R. Rivest à CRYPTO 90, sous le nom de MD4 (Actes du congrès CRYPTO 90, collection "Lecture Notes in Computer Science", pp. 303-311). On peut utiliser également la modification de cette méthode introduite avec le nom MD5 ou encore le standard américain SHA (secure hash standard, Federal Information Processing Standards Publications, 30 octobre 1992). Il est enfin possible d'utiliser à la place de la fonction de hachage un algorithme de chiffrement tel que DES, où le message à hacher joue le rôle de la clé et/ou du texte clair à chiffrer. On recommande cependant d'itérer un tel procédé de façon que le condensé obtenu par hachage ait de préférence au moins 128 bits.

Le dispositif d'identification utilise par ailleurs un générateur de permutations aléatoires permutant des vecteurs binaires. Un tel générateur peut être réalisé à partir d'une source de bruit blanc numérisée, par exemple une diode polarisée en inverse dans la zone dite "du coude", ou peut aussi être construit par des méthodes logicielles comme décrit dans les brevets américains 4 817 147 au nom de GUNTER ou 4 649 419 au nom d'ARAGON.

Selon un premier mode de réalisation du procédé d'authentification, dans une première étape commune aux différents procédés, le dispositif d'identification révèle au dispositif de vérification son identité et/ou sa clé publique signée.

D'autre part, après avoir choisi aléatoirement deux vecteurs U et V de dimensions respectives m et n constitués d'entiers compris entre 0 et d-1 ainsi que deux permutations p et q respectivement sur m et n éléments, le dispositif d'identification calcule et transmet au dispositif de vérification les engagements h1, h2 et h3 définis à partir d'un dispositif de hachage par $h1 = H(p,q,MU + P*V)$, $h2 = H(U.p,V.q)$ et $h3 = H((U + S).p, (V - T).q)$ où P*V désigne le produit terme à terme des composantes des vecteurs P et V, réduit modulo d et où T est le vecteur

k(M(S)), lequel peut être calculé en fonction de S par le dispositif d'identification ou stocké dans une partie physiquement inviolable de la mémoire du dispositif ;

- le dispositif de vérification tire d'une façon aléatoire un nombre b tel que $0 < b < 4$ ;

- si b vaut 1, alors le dispositif d'identification retourne une réponse r constituée des valeurs de p, q, U et V ;

- si au contraire b vaut 2, le dispositif d'identification retourne une réponse r constituée de p,q et des vecteurs $U' = (U + S)$, $V' = (V - T)$ ;

- si enfin b vaut 3, alors le dispositif retourne une réponse r constituée des vecteurs U.p, V.q ainsi que des vecteurs $U'' = (U + S).p$ et $V'' = (V - T).q$ ;

- le dispositif de vérification reçoit la réponse r, dans le cas $b = 1$, il calcule à partir des éléments reçus p, q, U, V, les valeurs de $MU + P*V$, U.p, V.q lesquelles doivent, si la réponse est correcte, être telles que $h1 = H(p,q,MU + P*V)$ ; $h2 = H(U.p, V.q)$ ;

- si au contraire $b = 2$, il calcule à partir des éléments reçus p,q U', V', les valeurs de $MU' + P*V'$, U'.p, V'.q lesquelles doivent, si la réponse est correcte, être telles que $h1 = H(p,q, MU' + P*V')$ et $h3 = H(U'.p, V'.q)$ ;

- si b vaut 3, alors le dispositif de vérification vérifie les deux égalités $h2 = H(U.p, V.q)$ et $h3 = H(U'', V'')$, de plus le dispositif de vérification calcule les deux vecteurs U'' - U.p et V'' - V.q et teste que ces vecteurs sont bien constitués uniquement d'éléments de X.

Selon un autre mode de réalisation privilégié de la présente invention, dans une première étape commune aux différents procédés, le dispositif d'identification révèle au dispositif de vérification son identité et/ou sa clé publique signée,

- puis après avoir choisi aléatoirement deux vecteurs U,V de tailles respectives m et n constituées d'entiers compris entre 0 et d-1 ainsi que deux permutations p et q respectivement sur m et n éléments, le dispositif d'identification transmet au dispositif de vérification les engagements h1 et h2 définis à partir du dispositif de hachage par $h1 = H(p,q,MU + P*V)$, $h2 = (U.p, V.q)$, où P*V désigne le produit terme à terme des composantes des vecteurs P et V réduits modulo d,

- le dispositif de vérification tire de façon aléatoire un nombre a compris entre 0 et d - 1 ;

- alors le dispositif d'identification calcule et envoie au dispositif de vérification les vecteurs Y = (aS + U).p et Z = (aT - V).q où T est le vecteur k(M(S)), lequel peut être calculé en fonction de S par le dispositif d'identification ou stocké dans une partie physiquement inviolable de la mémoire du dispositif ;

- le dispositif de vérification tire de façon aléatoire un bit b = 0 ou 1 ;

- si b vaut 0, alors le dispositif d'identification retourne une réponse r constituée des valeurs de p et q ;

- si au contraire b vaut 1, le dispositif retourne une réponse r constituée des vecteurs U' = S.p et V' = T.q ;

- le dispositif de vérification reçoit la réponse r, dans le cas b = 0, il calcule à partir de p et q les vecteurs X' et Z' tels que (Y').p = Y et (Z').q = Z, puis le vecteur M(Y') - P*Z' lequel doit si la réponse est correcte être tel que h1 = H(p,q,M(Y') - P*Z') ;

- si b = 1, alors le dispositif de vérification calcule les vecteurs Y - aU' et aV' - Z lesquels doivent si la réponse est correcte être tels que h2 = H(Y - aU', aV' - Z) et le dispositif de vérification teste de plus que les vecteurs U' et V' sont constitués uniquement d'éléments de X.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description de deux modes de réalisation du procédé, cette description étant faite avec référence aux dessins ci-annexés, dans lesquels :

- la figure 1 est un schéma expliquant un premier mode de mise en oeuvre du procédé d'authentification conforme à la présente invention, et

- la figure 2 est un schéma d'un second mode de réalisation du procédé conforme à la présente invention.

La présente invention concerne donc un nouveau procédé d'authentification réalisé par un protocole à apport nul de connaissance. Dans ce cas, la sécurité du procédé est basée sur le problème des équations linéaires contraintes. Ce problème consiste à trouver n valeurs satisfaisant un certain nombre d'équations linéaires modulo un nombre premier d, ces valeurs étant de plus contraintes à se trouver dans un

ensemble prescrit X. Le problème posé ci-dessus est en fait très difficile à résoudre par les moyens de calcul connus à ce jour dès que le nombre de variables est grand. Le système décrit correspond, en fait, au cas de m équations à n + m variables et, avec des valeurs m = n = 20, on dépasse déjà largement les possibilités des calculateurs.

Pour mettre en oeuvre le procédé d'authentification conforme à la présente invention, une autorité choisie et publie une matrice M de dimensions m x n, de préférence m = n, cette matrice étant constituée de coefficients choisis aléatoirement parmi les entiers compris entre 0 et d - 1. d est en général un nombre premier proche du carré d'un nombre c. De préférence, d = 257, à savoir (16 x 16) + 1. L'autorité choisit aussi une collection de vecteurs S de dimensions n dont les coordonnées sont choisies aléatoirement dans un ensemble X. L'ensemble X est déterminé en fonction d'un ensemble G appelé groupe multiplicatif formé de la suite des puissances successives d'un nombre réduites modulo d, cet ensemble étant choisi de façon que le nombre d'éléments de G soit c. Dans ce cas, il existe alors un ensemble X formé également de c éléments et tel que tout entier compris entre 1 et d-1 s'écrive de manière unique comme produit d'un élément de l'ensemble G et d'un élément de l'ensemble X. On notera donc g(u) l'élément de G intervenant dans l'unique décomposition d'un entier u compris entre 1 et d-1 et k(u) l'élément correspondant de X. Si U est un vecteur d'entiers compris entre 1 et d-1, g(u) est formé des images par G des coordonnées de U. On définit de même k(U).

La clé secrète ainsi déterminée est distribuée aux différents dispositifs d'identification. D'autre part, on publie l'ensemble des clés publiques constituées par le vecteur P = g(M (S)). Dans le cadre de la présente invention, cette clé publique peut être codée sur un faible nombre d'octets de même que la clé secrète S par l'intermédiaire d'une table des éléments de G et de X. Ainsi, dans le cas où d = 257 et où m = n = 20, on obtient des clés de 10 octets, ce qui constitue un avantage du présent procédé par rapport aux autres procédés à apport nul de connaissance connus à ce jour.

On décrira maintenant deux modes de réalisation spécifiques du procédé de la présente invention.

Le premier procédé sera décrit avec référence à la figure 1 qui représente schématiquement le protocole de communication mis en

oeuvre entre un dispositif d'identification et le dispositif de vérification, pour réaliser une authentification. Les dispositifs d'identification qui peuvent être constitués, par exemple, par des cartes à puces ou des clés électroniques doivent être physiquement inviolables. Ainsi, pour une carte à puce, il doit être impossible d'accéder à sa mémoire interne. Rien par contre n'est supposé concernant l'environnement dans lequel évolue le dispositif de vérification. D'autre part, le dispositif d'identification comporte dans une mémoire non volatile sa clé secrète S, à savoir le vecteur S de dimension n et la matrice M de dimension m x n tandis que le dispositif de vérification comporte dans une mémoire non volatile l'ensemble des clés publiques constituées des vecteurs P, ou bien des données suffisantes pour vérifier qu'une clé P signée a bien été produite par l'autorité compétente. Quand un dispositif d'identification veut entrer en contact avec un dispositif de vérification, les deux dispositifs exécutent le protocole suivant :

- tout d'abord le dispositif d'identification révèle son identité et/ou sa clé signée au dispositif de vérification qui vérifie que l'identité en question correspond bien à P ;

- ensuite le dispositif d'identification choisit deux vecteurs aléatoires U,V de tailles respectives m et n, de préférence m = n, constitués d'entiers compris entre 0 et d-1 ainsi que deux permutations aléatoires p et q, respectivement sur m et n éléments. Alors, le dispositif d'identification calcule les éléments suivants : h1 = H(p,q,MU + P*V), h2 = H(U.p, V.q) et h3 = H((U + S).p, (V-T).q) où P*V désigne le produit terme à terme des composantes des vecteurs P et V réduit modulo d et où T est le vecteur k(M(S)). Une fois le calcul effectué, le dispositif d'identification envoie au dispositif de vérification l'engagement h1, h2, h3. Alors, le dispositif de vérification tire de façon aléatoire un nombre b tel que $0 < b < 4$ et l'expédie au dispositif d'identification ;

- ensuite le dispositif d'identification calcule et envoie au dispositif de vérification une réponse r définie par :

- si b = 1, alors r est constituée des valeurs de p, q, U et V ;

- si b = 2, alors r est constituée de p,q et des vecteurs U' = (U + S) et V' = (V - T) ;

- si b = 3, alors r est constituée des vecteurs U.p, V.q et des vecteurs U" = (U + S).p et V" = (V - T).q.

Le dispositif de vérification reçoit la réponse r et,

- si b = 1, il calcule à partir des éléments reçus p,q, U,V les valeurs de MU + P*V, U.p, V.q, et ces valeurs doivent, si la réponse est correcte, être telles que h1 = H(p,q,MU + P*V), h2 = H(U.p, V.q) ;

- si b = 2, le dispositif de vérification calcule à partir des éléments reçus p,q, U', V' les valeurs de MU' + P*V', U'.p, V'.q et ces valeurs doivent, si la réponse est correcte, être telles que h1 = H(p,q,MU' + P*V), h3 = H(U'.p, V'.q) ;

- si b = 3, alors le dispositif de vérification vérifie les deux égalités h2 = H(U.p, V.q) et h3 = H(U".p, V".q). De plus, le dispositif de vérification calcule les deux vecteurs U" - U.p et V.q - S" et teste que ces vecteurs sont bien constitués uniquement d'éléments de l'ensemble X. Si le test ci-dessus s'est avéré correct, le dispositif de vérification considère que le protocole s'est terminé par un succès. Si le test n'est pas correct, le dispositif d'identification est rejeté.

Le dispositif de vérification répète les étapes ci-dessus un nombre t de fois, fonction du niveau de sécurité requis. Lorsque le dispositif est accepté, on envoit une impulsion de commande sur l'interface entrée/sortie du système protégé qui permet la mise en route de la transaction ultérieure.

L'ensemble des opérations ci-dessus est symbolisé sur la figure 1 dans laquelle la partie de gauche représente les différentes opérations réalisées au niveau du dispositif d'identification, tandis que la partie de droite représente les différentes opérations réalisées au niveau du dispositif de vérification, les flèches symbolisant l'envoi d'informations d'un dispositif vers l'autre.

Un autre mode de mise en oeuvre du procédé d'authentification de la présente invention sera maintenant décrit avec référence à la figure 2.

Ce second mode de réalisation demande plus de calculs que le mode de réalisation précédent, mais la probabilité de succès d'une entité illégale décroit plus vite. Ce mode de réalisation comporte donc les étapes suivantes, symbolisées sur la figure 2 de manière identique à la symbolisation utilisée sur la figure 1. Dans ce cas, le dispositif d'identification révèle au dispositif de vérification son identité ou sa clé publique signée de la même manière que dans l'autre mode de réalisation.

Puis après avoir choisi aléatoirement deux vecteurs V de tailles respectives m et n, (m pouvant être égal à n) constitués d'entiers compris entre 0 et d-1 ainsi que deux permutations p et q respectivement sur m et n éléments, le dispositif d'identification calcule les éléments suivants à savoir : h1 = H(p,q,MU + P*V), h2 = (U.p, V.q), ou P*V désigne le produit terme à terme des composantes des vecteurs P et V modulo d et H désigne une fonction de hachage cryptographique. Alors, l'engagement h1 et h2 est envoyé sur le dispositif de vérification. Le dispositif de vérification tire de façon aléatoire un nombre a compris entre 0 et d - 1 et l'envoie sur le dispositif d'identification.

Alors, le dispositif d'identification calcule et envoie au dispositif de vérification les vecteurs Y = (aS + U).p et Z = (aT - V).q où T est le vecteur k(M(S)) qui peut être calculé en fonction de S par le dispositif d'identification ou stocké dans une partie physiquement inviolable de la mémoire du dispositif.

Ensuite le dispositif de vérification tire de façon aléatoire un bit b qui peut être égal à 0 ou à 1 :

- si b = 0, alors le dispositif d'identification envoie une réponse r constituée des valeurs de p, q ;

- si b = 1, le dispositif d'identification envoie une réponse r constituée des vecteurs U' = S.p et V' = T.q ;

Le dispositif de vérification reçoit la réponse r et :

- si b = 0, il calcule à partir de p, q les vecteurs Y' et Z' tels que (Y').p = Y et (Z').q = Z puis le vecteur M(Y') - P*Z' qui, si la réponse est correcte, doit être tel que h1 = H(p,q,M (Y') - P*Z') ;

- si b = 1, alors le dispositif de vérification calcule les vecteurs Y - aU' et aV' - Z qui, si la réponse est correcte, doivent être tels que h2 = H(Y - aU', aV' - Z). Alors le dispositif de vérification teste, de plus, que les vecteurs U' et V' sont constitués uniquement d'éléments appartenant à l'ensemble X.

Si le test correspondant à b est correct, le dispositif de vérification considère que le protocole s'est terminé par un succès et le dispositif d'identification est accepté et on envoie une impulsion de commande sur l'interface entrée/sortie du système protégé qui permet la mise en route de la transaction ultérieure. Si le test n'est pas correct, le dispositif d'identification est rejeté.

Pour accroître la sécurité du procédé, les deux dispositifs d'identification et de vérification répètent les étapes ci-dessus plusieurs fois, à savoir t fois, le dispositif de vérification n'authentifiant le dispositif d'identification que si toutes les sessions du protocole se sont soldées par un succès. De préférence, on choisit t tel que $0 < t < 60$, les valeurs $t = 35$ et $t = 20$ constituant respectivement pour le premier et le second mode de réalisation, des exemples typiques apportant une sécurité suffisante pour nombre d'applications.

On a décrit ci-dessus deux modes de réalisation particuliers qui peuvent être modifiés sans sortir du cadre de la présente invention.

## REVENDICATIONS

1. Procédé d'authentification d'au moins un dispositif d'identification par un dispositif de vérification basé sur des techniques cryptographiques à clés secrètes et publiques, l'authentification étant réalisée par un protocole à apport nul de connaissance, caractérisé en ce que la clé publique est établie en utilisant les équations linéaires contraintes.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte les étapes suivantes :

- pour permettre le dialogue entre le dispositif d'identification et le dispositif de vérification, établir une clé secrète constituée par au moins un vecteur S de dimension n dont les coordonnées sont choisies dans un ensemble X fixé et une clé publique comprenant une matrice M de dimensions m x n dont les coefficients sont choisis aléatoirement parmi les entiers compris entre 0 et d-1 où d est un nombre premier proche du carré d'un nombre c, et au moins un vecteur P tel que $P = g(M(S))$ où g désigne une fonction qui est définie à partir de l'ensemble X et d'un sous groupe G de l'ensemble des entiers (1, 2..d-1) et qui associe à chaque coordonnée x d'un vecteur, un élément g(x) de G tel que x s'écrive d'une manière unique comme produit de g(x) et d'un élément k(x) de X,

- au niveau du dispositif d'identification, recevoir un ou plusieurs éléments aléatoires (U,V,p,q) produits par le dispositif de vérification et envoyer au dispositif de vérification un engagement obtenu en appliquant une fonction de hachage cryptographique sur des paramètres fonctions de S, de M et des éléments aléatoires tirés par le dispositif de vérification,

- puis, en fonction du ou des nombres aléatoires tirés par le dispositif de vérification, tester au niveau du dispositif de vérification à l'aide des éléments reçus et de la clé publique, que les engagements sont corrects.

3. Procédé selon l'une quelconque des revendications 1 et 2, caractérisé en ce que l'on répète les opérations précédentes un nombre de fois fonction du niveau de sécurité souhaité.

4. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que l'ensemble X est formé de c éléments tels que tout entier compris entre 1 et d-1 s'écrive de manière unique comme produit d'un élément de G et d'un élément de X.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que les éléments aléatoires sont constitués par deux vecteurs U et V de dimensions respectives m et n et constitués d'entiers compris entre 0 et d-1 et par deux permutations p et q respectivement sur m et n éléments.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce que $m=n$.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que $d = 257$ et $n=20$.

8. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que, au début de chaque dialogue, le dispositif d'identification révèle au dispositif de vérification son identité et/ou sa clé publique signée.

9. Procédé selon l'une quelconque des revendications 1 à 8, caractérisé en ce que, une fois le dialogue établi entre le dispositif d'identification et le dispositif de vérification et les éléments aléatoires choisis :

- le dispositif d'identification calcule et transmet au dispositif de vérification les engagements h1 et h2 définis à partir d'un dispositif de hachage par $h1=H(p,q,MU+P*V)$, $h2 = (U.p,V.q)$ où $P*V$ désigne le produit terme à terme des composantes des vecteurs P et V, réduit modulo d ;

- le dispositif de vérification tire d'une façon aléatoire un nombre a compris entre 0 et d-1 ;

- alors, le dispositif d'identification calcule et envoie au dispositif de vérification les vecteurs $Y=(aS+U).p$ et $Z=(aT-V).q$, où T est le vecteur k(M(S)) ;

- le dispositif de vérification tire de façon aléatoire un bit $b=0$ ou 1 ;

- si b vaut 0, alors le dispositif d'identification retourne une réponse r constituée des valeurs de p, q ;

- si b vaut 1, le dispositif d'identification retourne une réponse r constituée des vecteurs $U'=S.p$ et $V'=T.q$ ;

- le dispositif de vérification reçoit la réponse r, dans le cas $b=0$, il calcule, à partir de p et q les vecteurs Y' et Z' tels que $(Y').p=Y$ et $(Z').q=Z$, puis le vecteur $M(Y')-P*Z'$ lequel doit, si la réponse est correcte, être tel que $h1=H(p,q,M(Y')-P*Z')$ ;

- si maintenant $b=1$, alors le dispositif de vérification calcule les vecteurs Y-aU' et aV'-Z, lesquels doivent, si la réponse est correcte, être tels que $h2 = H(Y-aU',aV'-Z)$, le dispositif de vérification testant de plus que les vecteurs U' et V' sont constitués uniquement d'éléments de X.

10. Procédé selon l'une quelconque des revendications 1 à 8, caractèrisé en ce que, une fois le dialogue établi entre le dispositif d'identification et le dispositif de vérification et les éléments aléatoires choisis :

- le dispositif d'identification calcule et transmet au dispositif de vérification les engagements h1, h2 et h3 définis à partir d'un dispositif de hachage par $h1=H(p,q,MU+P*V)$, $h2=H(U.p,V.q)$ et $h3=H((U+S).p,(V-T).q)$ où $P*V$ désigne le produit terme à terme des composantes des vecteurs P et V, réduit modulo d et où T est le vecteur $k(M(S))$ ;

- le dispositif de vérification tire de façon aléatoire un nombre b tel que $0<b<4$ ;

- si b vaut 1, alors, le dispositif d'identification retourne une réponse r constituée des valeurs de p,q,U et V ;

- si b vaut 2, alors le dispositif retourne une réponse r constituée de p,q et des vecteurs $U'=(U+S)$ et $V'=(V-T)$ ;

- si b vaut 3, alors le dispositif retourne une réponse r constituée des vecteurs U.p, V.q ainsi que des vecteurs $U''=(U+S).p$ et $V''=(V-T).q$ ;

- le dispositif de vérification reçoit la réponse r, dans le cas $b=1$, il calcule à partir des éléments reçus p,q,U,V, les valeurs de $MU+P*V$, U.p, V.q lesquelles doivent, si la réponse est correcte, être telles que $h1=H(p,q,MU+P*V)$, $h2=H(U.p,V.q)$ ;

- si au contraire b vaut 2, il calcule à partir des éléments reçus p,q,U',V', les valeurs de $MU'+P*V'$, U'.p, V'.q lesquelles doivent, si la réponse est correcte, être telles que $h1=H(p,q,MU'+P*V')$ et $h3=H(U'.p,V'.q)$ ;

- si enfin b vaut 3, alors le dispositif de vérification vérifie les deux égalités h2 = H(U.p,V.q) et h3 = H(U'',V''), de plus, le dispositif de vérification calcule les deux vecteurs U"-U.p et V.q-V'' et teste que ces vecteurs sont bien constitués uniquement d'éléments de X.

11. Procédé selon l'une quelconque des revendications 9 et 10, caractérisé en ce que l'on répête les étapes ci-dessus un nombre t de fois, fonction du niveau de sécurité requis, le dispositif de vérification n'authentifiant le dispositif d'identification que si toutes les sessions du protocole se sont soldées par un succès.

12. Procédé selon l'une quelconque des revendications 9 et 10, caractérisé en ce que le vecteur k (M(S)) est calculé en fonction de S par le dispositif d'identification ou est stocké dans une partie physiquement inviolable de la mémoire du dispositif.

2714780

| DISPOSITIF D'IDENTIFICATION<br>Clé secrète = vecteurs S | INTERFACE DE COMMUNICATION ENTRE LES DEUX DISPOSITIFS | DISPOSITIF DE VERIFICATION<br>Clé publique = vecteur P |
|---|---|---|
| Produire :<br>- un vecteur aléatoire U de taille m<br>- un vecteur aléatoire V de taille n<br>- une permutation aléatoie p sur m<br>- une permutation aléatoire q sur n | | |
| Calculer : h1 = H(p,q,MU + P*V)<br>h2 = (U.p, V.q)<br>h3 = H((U + S).p, (V-T).q))<br>T = k (M(s)) | | |
| Envoyer h1, h2, h3 | | Recevoir h1, h2, h3 |
| | | produire un nombre aléatoire b tel que :<br>0< b< 4 |
| Recevoir b | | Envoyer b |
| si b = 1 alors r = {p, q, U, V}<br>si b = 2 alors r = {p, q, U' = U + S,<br>V' = V - T}<br>si b = 3 alors r' = {U.p, V.q<br>U''= (V + S).p,<br>V'' = (V - T).q} | | |
| Envoyer r | | Recevoir r |
| | | si b = 1 vérifier h1, h2 |
| | | si b = 2 vérifier h1, h3 |
| | | si b = 3 vérifier h2, h3 |
| | | et tester que les vecteurs trouvés<br>ε à X |

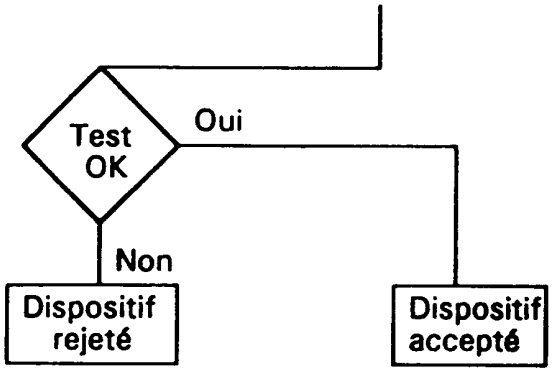



FIGURE 1

**DISPOSITIF D'IDENTIFICATION**
Clé secrète = vecteurs S

Produire :
- un vecteur aléatoire U de taille m
- un vecteur aléatoire V de taille n
- une permutation aléatoie p sur m
- une permutation aléatoire q sur n

Calculer : h1 = H(p,q,MU + P*V)
h2 = (U.p, V.q)

Envoyer h1, h2

Recevoir a

Calculer :
Y = (aS + U).p
Z = (aT - V).q
T = k (M(s))

Envoyer Y, Z

Recevoir b
si b = 0 alors r = {p,q}
si b = 1 alors r = {U' = S.p, V' = T.q}

Envoyer r

INTERFACE DE COMMUNICATION ENTRE LES DEUX DISPOSITIFS

**DISPOSITIF DE VERIFICATION**
Clé publique = vecteur P

Recevoir h1, h2
Tirer un nombre aléatoire a tel que :
0< a< d - 1
Envoyer a

Recevoir Y, Z
Tirer un nombre aléatoire b tel que :
0 < b < 1

Envoyer b

Recevoir r

si b = 0 vérifier h1

si b = 1 vérifier h2

et tester que les vecteurs Ɛ à X

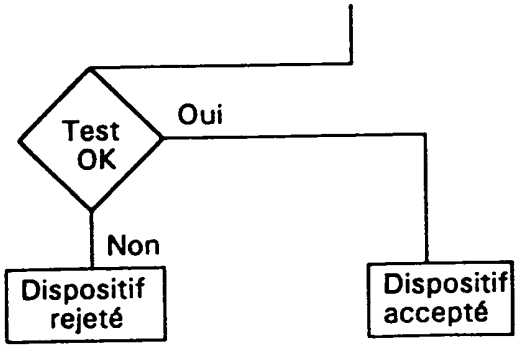



**FIGURE 2**

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

# RAPPORT DE RECHERCHE PRELIMINAIRE

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

2714780

N° d'enregistrement national

FA 496097
FR 9315879

| DOCUMENTS CONSIDERES COMME PERTINENTS | | Revendications concernées de la demande examinée |
|---|---|---|
| Catégorie | Citation du document avec indication, en cas de besoin, des parties pertinentes | |
| A | EP-A-0 252 499 (YEDA RESEARCH AND DEVELOPMENT COMPANY)<br>* page 3, ligne 46 - page 4, ligne 17 *<br>* figure 3 * | 1 |
| D,A | & US-A-4 748 668 (FIAT ET AL.) | 1 |
| | --- | |
| D,A | US-A-4 932 056 (SHAMIR)<br>* abrégé *<br>* colonne 2, ligne 65 - colonne 3, ligne 23 *<br>* figure 1 * | 1 |
| | --- | |
| D,A | ADVANCES IN CRYPTOLOGY - CRYPTO '93<br>22-26 August 1993, Santa Barbara (US)<br>NEW YORK (US)<br>pages 13-20;<br>J.STERN:<br>"A NEW IDENTIFICATION SCHEME BASED ON SYNDROME DECODING"<br>* page 13, ligne 11 - page 14, ligne 32 * | 1 |
| | ----- | |

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

H04L

| Date d'achèvement de la recherche | Examinateur |
|---|---|
| 9 Septembre 1994 | Lydon, M |

CATEGORIE DES DOCUMENTS CITES

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

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

& : membre de la même famille, document correspondant



EPO FORM 1503 03.82 (P04C13)