(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
13 mars 2003 (13.03.2003)

PCT

(10) Numéro de publication internationale
WO 03/021864 A2

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR02/03022

(22) Date de dépôt international :
5 septembre 2002 (05.09.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/11502 5 septembre 2001 (05.09.2001) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F-13420 Gemenos (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **CORON, Jean-Sébastien** [FR/FR]; 4, rue Léon Delagrange, F-75015 Paris (FR). **NACCACHE, David** [FR/FR]; 7, rue Chaptal, F-75009 Paris (FR).

(74) Mandataire : **PELLEGRINI, Marie-Claude**; Gemplus, BP 100, F-13881 Gemenos Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

WO 03/021864 A2

(54) **Title:** METHOD OF REDUCING THE SIZE OF AN RSA OR RABIN SIGNATURE

(54) **Titre :** PROCEDE DE REDUCTION DE LA TAILLE D'UNE SIGNATURE RSA OU RABIN

(57) **Abstract:** The RSA cryptographic algorithm is the most commonly used public key cryptographic algorithm. The invention consists in defining a method that can be used to reduce the size of the signatures to be transmitted and stored. The invention can be easily used in a chip card type of portable electronic component.

(57) **Abrégé :** L'algorithme de chiffrement RSA est l'algorithme de chiffrement à clef publique le plus utilisé. L'invention consiste à définir une méthode permettant de réduire la taille des signatures à transmettre et à mémoriser. L'invention est facilement utilisable dans un composant électronique portable de type carte à puce.

PROCEDE DE REDUCTION DE LA TAILLE D'UNE SIGNATURE RSA OU RABIN

La présente invention concerne un procédé de réduction de la taille d'une signature RSA ou Rabin.

Dans le modèle classique de la cryptographie à clef secrète, deux personnes désirant communiquer par l'intermédiaire d'un canal non sécurisé doivent au préalable se mettre d'accord sur une clé secrète de chiffrement K. La fonction de chiffrement et la fonction de déchiffrement utilisent la même clef K. L'inconvénient du système de chiffrement à clé secrète est que ledit système requiert la communication préalable de la clé K entre les deux personnes par l'intermédiaire d'un canal sécurisé, avant qu'un quelconque message chiffré ne soit envoyé à travers le canal non sécurisé. Dans la pratique, il est généralement difficile de trouver un canal de communication parfaitement sécurisé, surtout si la distance séparant les deux personnes est importante. On entend par canal sécurisé un canal pour lequel il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des clefs à travers un canal non sécurisé. Le

principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, une clef publique de chiffrement et une clef privée de déchiffrement. Il doit être calculatoirement infaisable de trouver la clef privée de déchiffrement à partir de la clef publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clef publique de chiffrement de la personne B. Seule la personne B possède la clef privée associée à sa clef publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

Un autre avantage de la cryptographie à clé publique sur la cryptographie à clé secrète est que la cryptographie à clef publique permet l'authentification par l'utilisation de signature électronique.

La première réalisation de schéma de chiffrement à clef publique fut mise au point en 1977 par Rivest, Shamir et Adleman, qui ont inventé le système de chiffrement RSA. La sécurité de RSA repose sur la difficulté de factoriser un grand nombre qui est le produit de deux nombres premiers. Depuis, de nombreux systèmes de chiffrement à clef publique ont été proposés, dont la sécurité repose sur différents problèmes calculatoires ; (cette liste n'est pas exhaustive).

- " Sac à dos " de Merckle-Hellman :

  Ce système de chiffrement est basé sur la difficulté du problème de la somme de sous-ensembles ;

- McEliece :

  Ce système de chiffrement est basé sur la théorie des codes algébriques. Il est basé sur le problème du décodage de codes linéaires ;

- ElGamal :

  Ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini ;

- Courbes elliptiques:

  Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques. L'avantage des systèmes de chiffrement à courbes elliptiques est qu'ils nécessitent une taille de clef plus petite que pour les autres systèmes de chiffrement.

Le système de chiffrement RSA est le système de chiffrement à clé publique le plus utilisé. Il peut être utilisé comme procédé de chiffrement ou comme procédé de signature. Le système de chiffrement RSA est utilisé dans les cartes à puce, pour certaines applications de celles-ci. Les applications possibles de RSA sur une carte à puce sont l'accès à des banques de données, des applications bancaires, des applications de paiements à distance comme par exemple la télévision à péage, la distribution d'essence ou le paiement de péages d'autoroute.

Le principe du système de chiffrement RSA est le suivant. Il peut être divisé en trois

parties distinctes qui sont :

1) La génération de la paire de clés RSA ;

2) Le chiffrement d'un message clair en un message chiffré, et

3) Le déchiffrement d'un message chiffré en un message clair.

La première partie est la génération de la clef RSA. Chaque utilisateur crée une clé publique RSA et une clé privée correspondante, suivant le procédé suivant en 5 étapes :

1) Générer deux nombres premiers distincts p et q de même taille ;

2) Calculer $n=pq$ et $\phi=(p-1)(q-1)$;

3) Sélectionner aléatoirement un entier e, $1<e<\phi$, tel que $pgcd(e, \phi)=1$;

4) Calculer l'unique entier d, $1<d<\phi$, tel que $e*d=1 \bmod \phi$;

5) La clé publique est (n,e); la clé privée est d ou (d,p,q).

Les entiers e et d sont appelés respectivement exposant de chiffrement et exposant de déchiffrement. L'entier n est appelé le module.

La seconde partie consiste au chiffrement d'un message clair noté m au moyen d'un algorithme avec $1<m<n$ en un message chiffré noté c qui est le suivant :

Calculer $c=m^e \bmod n$.

La troisième partie consiste au déchiffrement d'un message chiffré utilisant l'exposant privé d de déchiffrement au moyen d'un algorithme.

L'algorithme de déchiffrement d'un message chiffré noté c avec 1<c<n en un message clair noté m est le suivant :

Calculer m=c^d mod n.

Le système Rabin est semblable au système RSA, la différence étant que l'exposant public de chiffrement est fixé à 2, ou plus généralement un entier pair.

Les systèmes RSA ou Rabin peuvent également être utilisés pour générer des signatures électroniques. Le principe d'un schéma de signature électronique basé sur le système RSA peut généralement être défini en trois parties :

- La première partie étant la génération de la clef RSA ou Rabin, en utilisant le méthode décrite dans la première partie du système RSA ou Rabin décrite précédemment ;

- La deuxième partie étant la génération de la signature. Le procédé consiste à prendre en entrée le message M à signer, à lui appliquer un encodage utilisant une fonction μ pour obtenir la chaîne de caractère $\mu(M)$, et à appliquer le procédé de déchiffrement de la troisième partie du système RSA décrit précédemment. Ainsi, seule la personne possédant la clef privée peut générer la signature ;

- La troisième partie étant la vérification de la signature. Le procédé consiste à prendre en entrée le message M à signer et la signature s

à vérifier, à appliquer un encodage au message M en utilisant une fonction μ pour obtenir la chaîne de caractère $\mu(M)$, à appliquer à la signature s le procédé de chiffrement décrit dans la deuxième partie du système RSA, et à vérifier que le résultat obtenu est égal à $\mu(M)$. Dans ce cas, la signature s du message M est valide, et dans le cas contraire elle est fausse.

Il existe de nombreux procédés d'encodage utilisant différentes fonctions μ. Un exemple de procédé d'encodage est le procédé décrit dans le standard « ISO/IEC 9796-2, Information Technology - Security techniques - Digital signature scheme giving message recovery, Part 2 : Mechanisms using a hash-function, 1997 ». Un autre exemple de procédé d'encodage est le procédé d'encodage décrit dans le standard « RSA Laboboratories, PKCS#1 : RSA cryptography specifications, version 2.0, September 1998 ». Ces deux procédés d'encodage permettent de signer des messages de taille arbitrairement longue.

L'inconvénient des deux procédés d'encodage cités précédemment est qu'ils nécessitent la transmission d'une signature électronique dont la taille est aussi grande que celle du module RSA, soit typiquement 1024 bits. Si la signature est générée par un dispositif disposant d'un faible débit de transmission, la transmission de la signature sera lente car la signature est de grande taille. De plus, si une entité doit garder en mémoire un grand nombre de signatures,

la capacité de stockage à mettre en œuvre sera importante.

Le procédé de l'invention consiste à réduire la taille de la signature qui est transmise ou mémorisée. Le procédé de l'invention consiste en deux parties distinctes, la première étant la génération de la signature courte, la deuxième étant la vérification de la signature courte.

Le procédé de génération de la signature courte prend en entrée un message M et la clef privée d de l'utilisateur, et comprend les étapes suivantes :

1) Génération de la signature S du message M à l'aide de la clef privée d de l'utilisateur, suivant la méthode de génération d'une signature RSA ou Rabin décrite précédemment.

2) Calcul d'une partie S' de la signature S, ladite partie pouvant être une chaîne de bits inclue dans la signature S.

Le procédé de vérification de la signature courte prend en entrée un message M, la signature courte S' à vérifier, et la clef publique de l'utilisateur, et comprend les étapes suivantes :

1) Génération de la signature S du message M à partir du message M et de la signature courte S'.
2) Vérification de la signature S suivant le procédé de vérification de signature RSA ou Rabin décrit précédemment.

Le procédé de l'invention comprend deux variantes. Dans une première variante, la signature courte S' est dérivée de la signature S en ne gardant que les bits de poids forts de la signature S. De plus, la taille relative de la signature courte S' par rapport à celle de la signature S doit être supérieure à 1-1/e, où e est l'exposant public de chiffrement. Par exemple, lors de l'utilisation du système Rabin avec e=2, la taille de la signature courte S' doit être supérieure à la moitié de la taille de la signature S.

Préférentiellement, l'exposant public e est égal à 3.

Dans une deuxième variante, la signature courte S' est dérivée de la signature S en ne gardant que les bits de poids faibles de la signature S. De plus, la taille relative de la signature courte S' par rapport à celle de la signature S doit être supérieure à 1-1/e, où e est l'exposant public de chiffrement.

Lors de la vérification de la signature, si la signature S' a été correctement générée, la signature S' est telle que $S^e=\mu(M) \bmod N$ avec $S=S'.2^b+x$ dans la première variante, et $S=x.2^b+S'$ dans la deuxième variante, N étant un entier, l'entier b étant un paramètre fixé, et x étant un entier positif de taille inférieur à la taille de N divisée par e. La signature S' est donc telle que $(S'.2^b+x)^e=\mu(M) \bmod N$ dans la première variante et $(x.2^b+S')^e=\mu(M)$ modulo N dans la deuxième variante. Dans ces 2 cas, l'entier x est donc solution d'une équation polynomiale modulo N de degré e, et de plus l'entier x est de taille inférieure à la taille de N divisée par e. Dans l'article « Small

solutions to polynomial equations, and low exponent RSA vulnerabilities » publié dans Journal of Cryptology, 10, 1997, D. Coppersmith décrit une méthode permettant de résoudre une équation polynomiale de ce type.
En utilisant cette méthode, on retrouve donc l'entier x dans chacune des deux variantes du procédé, ce qui permet de retrouver la signature S. On vérifie ensuite la validité de la signature S à l'aide du procédé de vérification de signature RSA ou Rabin décrit précédemment.

L'avantage du procédé de génération et de vérification de signature courte de la présente invention est que la taille de la signature à transmettre est plus petite que dans le cas général : en effet, il est ainsi possible de ne transmettre que 512 bits de la signature au lieu de 1024 bits, du fait de la troncature de la signature. Il en résulte de meilleures performances dues à des temps de transmission plus faibles et donc une exécution plus rapide. Le procédé est aussi avantageux lorsqu'un grand nombre de signatures doivent être stockées. Cette invention présente un intérêt particulier pour les dispositifs électroniques portables de petite taille du type puce électronique.

REVENDICATIONS

1) Procédé de réduction de la taille d'une signature électronique de type RSA ou Rabin, ledit procédé étant constitué de deux parties distinctes, la première partie étant la génération de la signature courte S' suivant la méthode de génération d'une signature RSA ou Rabin prenant en entrée un message M et la clef privée de l'utilisateur, la deuxième partie étant la vérification de la signature courte prenant en entrée le message M, la clef publique de l'utilisateur et la signature courte S', caractérisé en ce que la vérification de la signature utilise un procédé de résolution d'une équation polynomiale modulo N de degré e où N est un entier et e l'exposant public de chiffrement, la solution de l'équation étant de taille inférieure à la taille de N divisée par e, ladite équation polynomiale étant soit de la forme $(S'.2^b+x)^e = \mu(M)$ modulo N soit de la forme $(x.2^b+S')^e = \mu(M)$ modulo N, où b est un entier fixé et x un entier positif de taille inférieur à la taille de N divisée par e.

2) Procédé de réduction de la taille d'une signature électronique de type RSA ou Rabin, selon la revendication 1, caractérisé en ce que la signature courte S' est dérivée de la signature S en ne gardant que les bits de poids forts de la signature S, la taille relative de la signature courte S' par rapport à celle de la signature S devant être supérieure à 1-1/e, où e est l'exposant public de chiffrement.

3) Procédé de réduction de la taille d'une

signature électronique de type RSA ou Rabin, selon la revendication 1, caractérisé en ce que la signature courte S' est dérivée de la signature S en ne gardant que les bits de poids faibles de la signature S, la taille relative de la signature courte S' par rapport à celle de la signature S devant être supérieure à 1-1/e, où e est l'exposant public de chiffrement.

4) Procédé de réduction de la taille d'une signature électronique de type Rabin suivant l'une quelconque des revendications précédentes, caractérisé en ce que l'exposant de chiffrement e est égal à 2.

5) Procédé de réduction de la taille d'une signature électronique de type RSA suivant l'une quelconque des revendications 1 à 3 caractérisé en ce que l'exposant de chiffrement e est égal à 3.

6) Procédé suivant l'une quelconque des revendications précédentes, caractérisé en ce qu'il utilise un dispositif électronique.

7) Procédé suivant la revendication 6, caractérisé en ce qu'il utilise un dispositif portable.

8) Procédé suivant l'une quelconque des revendications 6 ou 7 caractérisé en ce qu'il utilise une carte à puce.