(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 février 2003 (13.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/013053 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR02/02453

(22) Date de dépôt international : 11 juillet 2002 (11.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/10409 2 août 2001 (02.08.2001) FR

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

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **CORON, Jean-Sébastien** [FR/FR]; 4 rue Léon Delagrange, F-75015 PARIS (FR).

(74) Mandataire : **BRUN, Philippe**; GEMPLUS, Service brevets, 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, 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).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes 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, UZ, VN, YU, ZA, ZM, ZW, 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)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes 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, UZ, VN, YU, ZA, ZM, ZW, 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)*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

[Suite sur la page suivante]

(54) **Title:** METHOD FOR DETERMINING THE SIZE OF A RANDOM VARIABLE FOR AN ELECTRONIC SIGNATURE SCHEMA

(54) **Titre :** PROCEDE DE DETERMINATION DE LA TAILLE D'UN ALEA POUR UN SCHEMA DE SIGNATURE ELECTRONIQUE

(57) **Abstract:** The invention concerns a method for determining the size of a random variable used to generate an electronic signature in public key cryptosystems, said size being both minimal and enabling to guarantee a level of security equivalent to base cryptographic systems.

(57) **Abrégé :** La présente invention concerne un procédé de détermination de la taille d'un aléa utilisé pour générer une signature électronique dans les systèmes de cryptographie à clef publique, ladite taille étant à la fois minimale et permettant de garantir un niveau de sécurité équivalent avec les systèmes cryptographiques de base.

WO 03/013053 A1

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

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.

PROCEDE DE DETERMINATION DE LA TAILLE D'UN ALEA POUR UN SCHEMA DE SIGNATURE ELECTRONIQUE

La présente invention concerne un procédé de détermination de la taille d'un aléa utilisé pour générer une signature électronique dans les systèmes de la cryptographie à clef publique.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. 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 signature électronique d'un message est un nombre dépendant à la fois de la clef privée connue seulement de la personne signant le message, ainsi que du contenu du message à signer. Une signature électronique doit être vérifiable : il doit être possible pour une tierce personne de vérifier la validité de la signature, sans que la connaissance de la clé privée de la personne signant le message ne soit requise ; la vérification de la signature s'effectue à l'aide de la clef publique correspondante.

Il existe de nombreux schémas de signature électronique. Les plus connus sont :

- Schéma de signature RSA : c'est le schéma de signature électronique le plus largement utilisé. Sa sécurité est

basée sur la difficulté de la factorisation de grands nombres ;

- Schéma de signature Rabin : sa sécurité est aussi basée sur la difficulté de la factorisation de grands nombres ;
- Schéma de signature de type El-Gamal : sa sécurité est basée sur la difficulté du problème du logarithme discret ; le problème du logarithme discret consiste à déterminer, s'il existe, un entier x tel que $y=g^x$ avec y et g deux éléments d'un ensemble E possédant une structure de groupe ;
- Schéma de signature Schnorr : il s'agit d'une variante du schéma de signature de type El-Gamal.

Techniquement, deux types de schéma de signature électronique se distinguent :

- Schémas de signature électronique nécessitant le message original pour la vérification de la signature : on transmet donc le message et la signature séparément ;
- Schémas de signature électronique avec reconstitution du message : le message original est obtenu d'après la signature elle-même ; le message original n'étant pas nécessaire pour vérifier la signature, la taille totale de la signature est plus courte.

La première réalisation d'un schéma 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. Le système 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 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 d'un schéma de signature électronique basé sur le système RSA peut généralement être défini en trois parties :

- 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 k/2 bits, k étant un paramètre entier;

2) Calculer le nombre n tel que : $n=p*q$ 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.

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

- La deuxième partie est 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 $\mu(M)$. La signature S est alors donnée par :

$$S=\mu(M)^d \bmod N ;$$

Ainsi, seule la personne possédant la clef privée correspondant à l'exposant d peut générer la signature ;

- La troisième partie est 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 calculer

$$Y=S^e \bmod N$$

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 de ces procédés d'encodage précédemment décrits est qu'ils n'offrent pas forcément un niveau de sécurité comparable au système RSA.

Au contraire, il existe des procédés d'encodage qui offrent un niveau de sécurité équivalent au schéma RSA. Le plus connu d'entre eux est le schéma de signature PSS, acronyme anglais désignant « Probabilistic Signature Scheme », décrit en 1996 par Bellare et Rogaway dans la publication intitulée « The exact security of digital signatures - How to sign with RSA and Rabin » et publiée à la conférence Eurocrypt 1996. Le schéma de signature PSS est inclus dans de nombreux standards, incluant

- IEEE P1363, Standard Specifications For Public Key Cryptography: Additional Techniques ;
- PKCS #1 v2.1, RSA Cryptography Standard.

Le schéma de signature PSS permet de signer un message M de longueur arbitraire. Il existe aussi une variante du schéma PSS nommée PSS-R dans laquelle on retrouve le message au moment de la vérification de la signature. Il n'est alors plus nécessaire de transmettre le message avec la signature.

Le procédé de signature PSS fonctionne de la manière suivante :

pour signer un message M, on concatène au message un aléa r de taille k_0 bits, k_0 étant un paramètre déterminé préalablement. On applique ensuite à M||r une fonction de hachage H qui renvoie en sortie une chaîne de taille k_1 bits, k_1 étant un paramètre, pour obtenir le résultat w. On définit une fonction de hachage G prenant en entrée un message de taille k_1 bits et renvoyant en sortie un message de taille $k-k_1-1$ bits. On définit la fonction G_1 qui renvoie les k_0 premiers bits de la fonction G, ainsi que la fonction G_2 qui renvoie les $k-k_1-k_0-1$ bits restants.

La fonction d'encodage $\mu(M)$ est alors donnée par :

$$\mu(M) = 0||w||G_1(w) \text{ xor } r||G_2(w).$$

Pour vérifier la signature S d'un message M, on calcule dans un premier temps

$$Y = S^e \bmod N$$

Et on écrit ensuite Y sous la forme $Y=0||w||r^*||g$, où w est une chaîne de taille k_1 bits, r^* est une chaîne de taille k_0 bits, et g est une chaîne comprenant les $k-k_0-k_1-1$ bits restants. On calcule $r=G_1(w)$ xor r^* et on vérifie que $w=H(M||r)$ et $g=G_2(w)$.

Le schéma de signature PSS-R, acronyme anglais désignant Probabilistic Signature Scheme - Recovery, est analogue au schéma PSS, la

différence étant qu'il permet de retrouver le message au moment de la vérification de la signature. La taille du message qui est retrouvée lors de la vérification de la signature est de $k-1-k_0-k_1$. On en déduit que plus la taille k_0 de l'aléa est petite, plus on peut retrouver un grand message lors de la vérification de la signature. On diminue donc ainsi la taille totale des données échangées : on n'a pas besoin de transmettre le message car il sera retrouvé au moment de la vérification de la signature. Or la taille des données échangées est cruciale dans beaucoup d'applications disposant de peu de mémoires, comme la carte à puce ou les ordinateurs de poches.

L'invention consiste en un procédé permettant de déterminer la taille optimale de l'aléa utilisé lors de la génération de la signature.

La taille est optimale au sens où elle est la taille minimale permettant de garantir un niveau de sécurité équivalent à RSA. L'utilisation d'un aléa de taille plus petite ne permet pas d'avoir un niveau de sécurité équivalent à celui de RSA.

Le procédé de l'invention est particulièrement destiné à s'appliquer au schéma de signature PSS, mais il peut s'étendre à d'autres schémas de signature aux caractéristiques analogues à PSS, par exemple au schéma de signature PFDH, acronyme anglais de « Probabilistic Full Domain Hash ». Le schéma PFDH fonctionne de la manière suivante. Pour générer une signature d'un message M, on concatène au message M un aléa r de taille k_0 bits, k_0 étant un paramètre déterminé préalablement. On applique

ensuite à M||r une fonction de hachage H qui renvoie en sortie une chaîne de taille k bits notée $\mu(M)=H(M||r)$.

Dans une première variante, le procédé consiste à inclure un compteur qui limite le nombre total de signature qui seront générées pour une clef publique donnée. Initialement, le compteur est fixé à zéro. A chaque nouvelle signature, on incrémente le compteur. Lorsque la valeur du compteur a dépassé une valeur maximale notée qsig, on ne peut plus générer de signature. On détermine alors la valeur optimale de la taille k_0 de l'aléa en déterminant k0=log(qsig)/log(2), où log désigne la fonction logarithme. L'avantage de cette première variante est que la taille k_0 de l'aléa est optimale : une taille k_0 inférieure à cette valeur engendrerait un niveau de sécurité inférieur au niveau de sécurité du système RSA, tandis qu'une taille k_0 supérieure à cette valeur diminuerait la taille du message qui peut être retrouvé lors de la vérification de la signature.

Dans une deuxième variante, le procédé consiste à utiliser le temps tgen nécessaire à la génération d'une signature, ainsi que la durée de vie maximale tvie du système de génération de signatures selon une clé publique donnée. Par exemple, une carte bancaire utilisant ce dit système de génération de signatures selon une clé publique donnée devant être renouvelée tous les deux ans possède une durée de vie tvie=2 ans.
On obtient alors le nombre maximal qsig de signatures pouvant être générées en calculant :

qsig=tvie/tgen.
On obtient ensuite suivant le même procédé décrit dans la première variante la taille optimale k_0 de l'aléa en calculant :
k0=log(qsig)/log(2)
L'avantage de cette deuxième variante est que l'on obtient un niveau de sécurité équivalent au système RSA, avec une taille de message retrouvé maximale, et sans utiliser de compteur.

Dans une troisième variante, on utilise un compteur q du nombre de signatures générées, mais on ne connaît pas à priori la valeur limite de ce compteur. Initialement, le compteur q est fixé à zéro, et la valeur du paramètre k_0 est fixée à zéro. A chaque nouvelle génération d'une signature, on incrémente le compteur q.
On détermine alors une nouvelle valeur de k_0 égale à la taille mesurée en nombre de bits de q. Par exemple, si q=7, k0=3, et si q=8, k0=4. L'avantage du procédé de la troisième variante est que l'on conserve tout au long du procédé une valeur optimale pour la taille k_0 de l'aléa : on conserve un niveau de sécurité équivalent au système RSA tout en permettant de retrouver une taille maximale de message.

Les schémas de signature utilisés pour la présente invention sont préférentiellement du RSA, Rabin, PSS, PSS-R et PFHD comme décrits précédemment dans la description.

Les trois variantes du procédé précédemment décrites mais non exhaustives peuvent s'appliquer plus généralement à tout système de signature dans lequel on retrouve la valeur de l'aléa au moment de la vérification de la signature. L'application de l'une quelconque des trois variantes du procédé précédemment décrites permettent d'obtenir une taille d'aléa généré optimale. Les trois variantes sont particulièrement destinées à être utilisées dans un objet portable électronique de type carte à puce.

REVENDICATIONS

1) Procédé de détermination de la taille d'un aléa utilisé dans la génération d'une signature électronique, ladite taille étant à la fois minimale et permettant de garantir un niveau de sécurité équivalent avec le système cryptographique de base utilisé à clé publique, caractérisé en ce que ledit procédé nécessite la connaissance du nombre total qsig de signatures qui sont générées pour une clef publique donnée, la taille k_0 de l'aléa étant déterminée par la formulation : $k_0=\log(qsig)/\log(2)$, log désignant la fonction logarithme.

2) Procédé selon la revendication 1 caractérisé en ce qu'il utilise un compteur du nombre de signatures générées, ledit compteur étant fixé initialement à zéro, ledit compteur étant incrémenté à chaque nouvelle génération de signature, le nombre total de signature pouvant être générées étant limité par un paramètre qsig fixé à l'avance, la taille k_0 de l'aléa généré étant déterminé par la formulation : $k_0=\log(qsig)/\log(2)$, log désignant la fonction logarithme.

3) Procédé selon la revendication 1 caractérisé en ce qu'une durée de vie tvie maximale d'un système de génération de signatures pour une clé publique donnée et un temps de génération

tgen d'une signature sont connus, le nombre maximal de signatures pouvant être générées est déterminé par la formulation : qsig=tvie/tgen, la taille k_0 de l'aléa généré est déterminée par k_0=log(qsig)/log(2), log désignant la fonction logarithme.

4) Procédé de détermination de la taille d'un aléa utilisé dans la génération d'une signature électronique, ladite taille étant à la fois minimale et permettant de garantir un niveau de sécurité équivalent avec le système cryptographique de base utilisé, caractérisé en ce qu'il utilise un compteur q du nombre de signatures, ledit compteur q étant fixé initialement à zéro, ledit compteur q étant incrémenté à chaque génération d'une signature, la taille k0 de l'aléa étant initialement fixée à 0, ladite taille k0 de l'aléa étant ensuite donnée par la taille mesurée en nombre de bits du compteur q.

5) Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit système cryptographique de base est RSA.

6) Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que ledit système cryptographique de base est Rabin.

7) Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le schéma de signature utilisé est PSS.

8) Procédé, selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le schéma de signature utilisé est PSS-R.

9) Procédé selon l'une quelconque des revendications 1à 4, caractérisé en ce que le schéma de signature utilisé est PFDH.

10) Procédé selon l'une quelconque des revendications 1à 9, caractérisé en ce qu'il est mis en œuvre dans un objet électronique portable.

11) Procédé selon la revendication précédente 9, caractérisé en ce que ledit dispositif électronique est une carte à puce.

12) Dispositif électronique portable mettant en oeuvre le procédé selon l'une quelconque des revendications 1 à11.

INTERNATIONAL SEARCH REPORT

Inte ıal Application No
PCT/FR 02/02453

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BELLARE M ET AL: "THE EXACT SECURITY OF DIGITAL SIGNATURES - HOW TO SIGN WITH RSA AND RABIN" ADVANCES IN CRYPTOLOGY - EUROCRYPT '96. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. SARAGOSSA, MAY 12 - 16, 1996, ADVANCES IN CRYPTOLOGY - EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CR, 12 May 1996 (1996-05-12), pages 399-416, XP000725449 ISBN: 3-540-61186-X page 402, line 17 -page 403, line 8 page 407, last paragraph -page 409, line 14 page 412, line 1 - last line --- -/--	1,4

[X] Further documents are listed in the continuation of box C. [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 December 2002	23/12/2002
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
P,X	CORON J-S: "OPTIMAL SECURITY PROOFS FOR PSS AND OTHER SIGNATURE SCHEMES" ADVANCES IN CRYPTOLOGY - EUROCRYPT 2002. INTERNATIONAL CONF. ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES. AMSTERDAM, NL, APRIL 28 - MAY 2, 2002, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN: SPRINGER, DE, vol. 2332, 28 April 2002 (2002-04-28), pages 272-287, XP001090352 ISBN: 3-540-43553-0 the whole document	1,3-5,7, 9

RAPPORT DE RECHERCHE INTERNATIONALE

Dem nternationale No
PCT/FR 02/02453

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, EPO-Internal, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	BELLARE M ET AL: "THE EXACT SECURITY OF DIGITAL SIGNATURES - HOW TO SIGN WITH RSA AND RABIN" ADVANCES IN CRYPTOLOGY - EUROCRYPT '96. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. SARAGOSSA, MAY 12 - 16, 1996, ADVANCES IN CRYPTOLOGY - EUROCRYPT. INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATION OF CR, 12 mai 1996 (1996-05-12), pages 399-416, XP000725449 ISBN: 3-540-61186-X page 402, ligne 17 -page 403, ligne 8 page 407, dernier alinéa -page 409, ligne 14 page 412, ligne 1 - dernière ligne --- -/--	1,4

[X] Voir la suite du cadre C pour la fin de la liste des documents

[ ] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
13 décembre 2002	23/12/2002

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
P,X	CORON J-S: "OPTIMAL SECURITY PROOFS FOR PSS AND OTHER SIGNATURE SCHEMES" ADVANCES IN CRYPTOLOGY - EUROCRYPT 2002. INTERNATIONAL CONF. ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES. AMSTERDAM, NL, APRIL 28 - MAY 2, 2002, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN: SPRINGER, DE, vol. 2332, 28 avril 2002 (2002-04-28), pages 272-287, XP001090352 ISBN: 3-540-43553-0 le document en entier	1,3-5,7, 9