(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 875 355**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **04 09766**

(51) Int Cl[8] : **H 04 L 9/06** (2006.01), G 06 F 17/10, G 06 K 19/073

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 15.09.04.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 17.03.06 Bulletin 06/11.

(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) :** *OBERTHUR CARD SYSTEMS SA Société anonyme* — FR.

(72) **Inventeur(s) :** BOSCHER ARNAUD et NACIRI ROBERT.

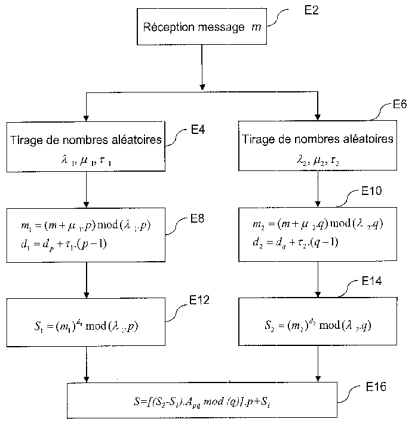
(73) **Titulaire(s) :**

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

(54) PROCEDE DE TRAITEMENT DE DONNEES, ENTITE ELECTRONIQUE ET CARTE A MICROCIRCUIT, NOTAMMENT POUR DECHIFFRER OU SIGNER UN MESSAGE DE FACON SECURISEE.

(57) Un procédé de traitement de données, ou une entité électronique associée transforme un premier message (m) en un second message (S) au moyen d'une clé privée composée d'un exposant et de deux nombres premiers (p,q), par exponentiation modulaire du premier message (m) audit exposant (d) modulo le produit des deux nombres premiers (p,q). Le procédé comprend les étapes suivantes:

- pour chaque nombre prernier (p;q), obtention d'un résultat modulaire (S_1;S_2) incluant une étape d'exponentiation modulaire à un exposant (d_1;d_2) dépendant dudit exposant (d), le résultat modulaire étant masqué pour l'un au moins des deux nombres premiers (p,q);
- obtention du second message (S) par recombinaison des résultats modulaires (S_1,S_2).



FR 2 875 355 - A1

L'invention concerne un procédé de traitement de données, une entité électronique et une carte à microcircuit, notamment pour déchiffrer ou signer un message au moyen d'une clé privée dans un système de chiffrement type RSA (pour Rivest-Shamir-Adleman), et ce de façon sécurisée.

Le système de chiffrement RSA est basé sur l'utilisation d'une clé publique formée de deux entiers (n, e) et d'une clé privée composée de trois entiers (d, p, q), tels que :

$n = p.q$ et $d.e = 1 \bmod [(p-1)(q-1)]$, où p et q sont des nombres premiers.

La sécurité de ce système est basée sur le fait qu'il est pratiquement impossible dans un temps limité d'obtenir la factorisation de n sous la forme $p.q$, c'est-à-dire d'obtenir la clé privée à partir de la clé publique.

L'application de la clé privée peut être utilisée dans les deux cas suivants :

- pour le déchiffrement d'un message issu d'un message original m et chiffré par exponentiation modulaire au moyen de la clé publique ($c = m^e \bmod n$): le déchiffrement est obtenu par la formule $m = c^d \bmod n$;

- pour la signature d'un message m selon la formule $s = m^d \bmod n$, la vérification de la signature pouvant alors être effectuée par un détenteur de la clé publique au moyen de la formule $m = s^e \bmod n$.

Dans les deux cas, l'application de la clé privée revient donc à l'exponentiation modulaire avec l'exposant de la clé privée d.

Le détenteur de la clé privée ayant connaissance de la factorisation $p.q$ du module public n, il a été proposé d'alléger le calcul d'exponentiation modulaire en utilisant le Théorème des Restes Chinois (souvent dénommé CRT de l'anglais *Chinese Reminder Theorem*). Cette technique permet d'effectuer les calculs sur des nombres de l'ordre de grandeur de p et de q (qui sont en général tous deux du même ordre de grandeur), c'est-à-dire sur des nombres

d'une longueur moitié par rapport à des nombres d'ordres de grandeur *n*, ce qui permet en théorie de réduire les calculs par un facteur quatre.

La technique utilisant le Théorème des Restes Chinois ou CRT se décompose en trois parties principales :

- la réduction initiale du message *m* en deux résidus modulaires relativement à *p* et à *q* ;
- un calcul d' exponentiation pour chaque résidu modulaire ;
- la recombinaison des résultats obtenus pour chaque résidu modulaire à l'étape précédente.

Des études ont été menées pour vérifier la fiabilité de cette technique sur le plan de la sécurité, comme expliqué par exemple dans l'article "*Attacking unbalanced RSA-CRT using SPA*" de Pierre-Alain FOUQUE, Gwenaëlle MARTINET et Guillaume POUPARD dans CHES 2003, LNCS 2779, pp. 254-268 (C.D. Walter et al., Springer-Verlag Berlin Heildelberg 2003).

Des contre-mesures ont été élaborées pour répondre aux différents types d'attaque envisageables, et notamment à celles décrites dans l'article susmentionné. Parmi ces contre-mesures sont prévus des techniques dites de masquage, qui consiste à modifier les valeurs mises en jeu lors des calculs cryptographiques d'une manière telle que le résultat du calcul n'en soit pas affecté.

Dans cet ordre d'idées, le document WO 03/023605 propose d'introduire une composante aléatoire dans les exposants utilisés lors du calcul d'exponentiation modulaire. Cette solution ne permet toutefois de modifier qu'une partie très réduite des valeurs mises en jeu lors du calcul, ce qui n'est pas satisfaisant sur le plan de la sécurité. Notamment, les résultats modulaires obtenus par exponentiation modulaire ne sont pas masqués puisqu'ils sont réduits modulo *p* et *q*.

Un autre type de masquage utilisé consiste, éventuellement en combinaison avec la solution qui vient d'être exposée, à effectuer non des calculs modulo *p* et modulo *q* respectivement, mais modulo des multiples entiers de *p* et de *q*. Ces multiples peuvent d'ailleurs être déterminés par tirage de nombres aléatoires.

Cette dernière solution est par exemple proposée dans l'article précité et dans les demandes de brevet WO 99/35782 (pages 20 à 23) et WO 01/28153.

Ces méthodes de masquage sont efficaces mais travaillent modulo des multiples de *p* et de *q*, et donc avec des nombres de dimensions supérieures. Après recombinaison des résultats obtenus respectivement modulo un multiple de *p* et modulo un multiple de *q*, le résultat de la recombinaison semblait a priori obtenu modulo un multiple de *n*, et on procédait de ce fait dans l'art antérieur à une réduction de ce résultat modulo *n* pour obtenir le résultat définitif de l'algorithme. Cette dernière étape qui utilise le nombre *n* rendait nécessaire un dimensionnement plus important de l'électronique que celui permis par l'utilisation du CRT et/ou allongeait le temps de traitement pour aboutir au résultat définitif.

Allant contre ce préjugé, les inventeurs se sont rendus compte que cette réduction modulo *n* était inutile et qu'ils pouvaient ainsi proposer un procédé de traitement de données transformant un premier message en un second message au moyen d'une clé privée composée d'un exposant et de deux nombres premiers, le second message étant le résultat d'une exponentiation modulaire du premier message audit exposant modulo le produit des deux nombres premiers, caractérisé en ce qu'il comprend les étapes suivantes :

- pour chaque nombre premier, obtention d'un résultat modulaire incluant une étape d'exponentiation modulaire à un exposant dépendant dudit exposant, le résultat modulaire étant masqué pour l'un au moins des deux nombres premiers ;

- obtention du second message par recombinaison des résultats modulaires.

L'étape de réduction modulo *n* prévue dans l'art antérieur étant supprimée, on réduit le temps de traitement et/ou le dimensionnement de l'électronique nécessaire à l'obtention du second message tout en bénéficiant de la sécurité fournie par l'utilisation d'un résultat modulaire masqué.

La recombinaison est par exemple réalisée par une combinaison d'additions modulaires et de multiplications modulaires. Ainsi, aucune division n'est utilisée ce qui permet de réduire le temps de traitement et/ou le dimensionnement de l'électronique.

La recombinaison des résultats modulaires peut utiliser pour modules les deux nombres premiers ; on utilise ainsi une formule classique de recombinaison.

Le procédé peut comprendre en pratique, pour chaque nombre premier, une étape de réduction d'un nombre dépendant du premier message modulo le produit du nombre premier et d'un entier associé, afin d'obtenir un résidu modulaire, et/ou, pour chaque nombre premier, une étape d'exponentiation modulaire du résidu modulaire, à un exposant dépendant dudit exposant, modulo le produit du nombre premier et de l'entier associé, afin d'obtenir le résultat modulaire.

En pratique, la recombinaison des résultats modulaires peut comprendre les étapes suivantes :

- soustraction du résultat modulaire obtenu pour un premier nombre premier au résultat modulaire obtenu pour le second nombre premier afin d'obtenir une différence ;
- multiplication de la différence par l'inverse modulaire du premier nombre premier modulo le second nombre premier afin d'obtenir un produit ;
- réduction du produit modulo le second nombre premier et multiplication du résultat de cette réduction par le premier nombre premier afin d'obtenir une valeur ;
- addition de cette valeur au résultat modulaire obtenu pour le premier nombre premier afin d'obtenir le second message.

Selon une possibilité de mise en œuvre, pour au moins un nombre premier, l'entier associé est déterminé par tirage de nombres aléatoires. Le masquage des valeurs utilisées lors du calcul est alors particulièrement sûr.

Le premier message est par exemple un message chiffré par la clé publique associée à la clé privée composée de l'exposant et des deux nombres premiers.

Le second message peut également être une signature obtenue au moyen de la clé privée. Le premier message peut alors être obtenu par concaténation de données.

L'invention propose également une entité électronique permettant la transformation d'un premier message en un second message au moyen d'une clé privée composée d'un exposant et de deux nombres premiers, le second message étant le résultat d'une exponentiation modulaire du premier message audit exposant modulo le produit des deux nombres premiers, caractérisée en ce qu'elle comprend :

- des moyens d'obtention, pour chaque nombre premier, d'un résultat modulaire incluant des moyens d'exponentiation modulaire à un exposant dépendant dudit exposant et aptes à générer un résultat modulaire masqué pour l'un au moins des deux nombres premiers ;
- des moyens d'obtention du second message par recombinaison des résultats modulaires.

Les modes possibles de réalisation et les avantages associés pour l'entité électronique correspondent à ceux du procédé évoqué ci-dessus.

L'invention propose enfin une carte à microcircuit comprenant une telle entité électronique. Cette entité électronique est par exemple portable, auquel cas il peut s'agir d'un assistant personnel numérique (ou PDA de l'acronyme anglo-saxon signifiant *"Personal Digital Assistant"*). Il peut également s'agir d'un passeport électronique qui contient une telle entité électronique associée à un système de communication radiofréquence. En variante, l'entité électronique peut être un module de sécurité (ou SHM de l'anglais *"Security Hardware Module"*) ou un ordinateur personnel (ou PC de l'anglais *"Personal Computer"*).

D'autres caractéristiques et avantages de la présente invention apparaîtront mieux à la lecture de la description qui suit, faite en référence aux dessins annexés, dans lesquels :

– la figure 1 représente schématiquement les éléments principaux d'une forme de réalisation possible pour une carte à microcircuit ;

– la figure 2 représente l'allure physique générale de la carte à microcircuit de la figure 1 ;

– la figure 3 représente un procédé réalisé conformément aux enseignements de l'invention.

La carte à microcircuit 10 dont les principaux éléments électroniques sont représentés à la figure 1 comporte un microprocesseur 2 relié d'une part à une mémoire vive (ou RAM de l'anglais *Random Access Memory*) 4 et d'autre part à une mémoire à semi-conducteur réinscriptible 6, par exemple une mémoire morte effaçable et programmable électriquement (ou EEPROM de l'anglais *Electrically Erasable Programable Read Only Memory*). En variante, la mémoire réinscriptible à semi-conducteur 6 pourrait être une mémoire flash.

Les mémoires 4, 6 sont reliées au microprocesseur 2 par un bus chacune sur la figure 1 ; en variante, il pourrait s'agir d'un bus commun.

La carte à microcircuit 10 comporte également une interface 8 de communication avec un terminal utilisateur réalisée ici sous forme de contacts dont un assure par exemple une liaison bidirectionnelle avec le microprocesseur 2. L'interface 8 permet ainsi l'établissement d'une communication bidirectionnelle entre le microprocesseur 2 et le terminal utilisateur dans lequel la carte à microcircuit 10 sera insérée.

Ainsi, lors de l'insertion de la carte à microcircuit 10 dans un terminal utilisateur, le microprocesseur 2 va mettre en œuvre un procédé de fonctionnement de la carte à microcircuit 10, selon un jeu d'instructions, stockées par exemple dans une mémoire morte (ou ROM de l'anglais *Read-Only Memory*) – non representée – ou dans la mémoire réinscriptible 6, qui définit un programme d'ordinateur. Ce procédé inclut en général l'échange de données avec le terminal utilisateur *via* l'interface 8 et le traitement de données au sein de la carte à microcircuit 10, et précisément au sein du microprocesseur 2 avec utilisation éventuelle de données stockées dans la mémoire réinscriptible 6 et de données stockées temporairement dans la mémoire vive 4.

Un exemple d'un tel procédé qui met en œuvre l'invention est donné dans la suite en référence à la figure 3.

La figure 2 représente l'allure physique générale de la carte à microcircuit 10 réalisée avec la forme générale d'un parallélépipède rectangle de très faible épaisseur.

L'interface de communication 8 pourvue des contacts déjà mentionnés apparaît clairement sur la face de la carte à microcircuit 10 visible sur la figure 2, sous forme d'un rectangle inscrit dans la face supérieure de la carte à microcircuit 10.

La figure 3 représente un mode possible de mise en œuvre du procédé de traitement de données selon l'invention.

A l'étape E2, le microprocesseur 2 reçoit le message m à traiter. On entend ici par message un nombre qui représente une information à transmettre ou le résultat obtenu par application à cette information d'une fonction de hachage (par exemple du type SHA-1 ou MD-5) en vue de sa signature. Dans le cas où l'unité de traitement est une carte à microcircuit comme décrit ci-dessus, le message m est par exemple reçu du terminal qui reçoit la carte via l'interface 8.

Le message m va ensuite être traité comme décrit ci-dessous selon les étapes E4 à E16. Bien que les étapes E4 à E14 soient représentées en deux branches sur la figure 3 (chacune des branches regroupant respectivement les étapes E4, E8, E12 et E6, E10, E14) afin de clarifier l'exposé, elles peuvent être réalisées successivement, par exemple dans l'ordre de numération des étapes.

Le procédé qui va être décrit ci-dessous permet d'obtenir la signature du message *m* par application d'une clé privée (*d, p, q*) conformément à l'algorithme RSA.

Si le message *m* était un message chiffré, un procédé analogue à celui qui va être décrit permettrait donc de déchiffrer le message *m* au moyen de cette clé privée.

On rappelle ici que les nombres *p* et *q* sont des nombres entiers qui constituent les facteurs premiers du module public (ou module de la clé publique) *n*. Ces nombres sont utilisés comme modules dans les calculs intermédiaires utilisant le Théorème des Restes Chinois sans masquage.

Le nombre *d* est quant à lui l'exposant de la clé privée qui est lié à l'exposant *e* de la clé publique par la relation : $d.e = 1 \bmod [(p-1)(q-1)]$.

Dans l'exemple décrit à la figure 3, on utilise trois entiers λ_1, μ_1, τ_1 pour les calculs relatifs au module *p*. Les entiers précités sont par exemple obtenus par tirage de nombres aléatoires, ce qui améliore encore comme précisé ci-dessous la sécurité du système. Naturellement, on entend ici par "*tirage de nombres aléatoires*" l'obtention de nombres pseudo-aléatoires par des techniques classiques dans ce domaine.

De manière analogue, on détermine à l'étape E6 trois entiers λ_2, μ_2, τ_2 utilisés pour les traitements relatifs au module *q*. Comme indiqué en ce qui concerne les entiers λ_1, μ_1, τ_1, les entiers λ_2, μ_2, τ_2 peuvent être obtenus par tirage de nombres aléatoires.

On passe alors à l'étape E8 qui regroupe les opérations de masquage des valeurs utilisées pour l'exponentiation modulaire relative au module *p*.

Pour ce faire, on calcule tout d'abord un premier message masqué m_1 selon la formule $m_1=(m+\mu_1.p) \bmod (\lambda_1.p)$.

On remarque que cette opération consiste d'une part à masquer le message lui-même en lui ajoutant un multiple entier du module *p* ($\mu_1 p$) et d'autre part à masquer le module *p* lui-même en le multipliant par un entier λ_1.

On comprend ainsi que, comme indiqué précédemment, l'utilisation d'entiers λ_1 et μ_1 obtenus par tirage de nombres aléatoires rend le masquage plus efficace et améliore ainsi la sécurité du système.

L'étape E8 comporte également une opération de calcul d'un exposant masqué $d_1=d_p+\tau_1.(p-1)$, où $d_p = d \bmod (p-1)$.

Cette dernière opération permet de masquer l'exposant utilisé lors de l'exponentiation modulaire comme indiqué plus bas.

On procède ensuite à l'étape E10 qui effectue des calculs analogues à ceux de l'étape E8, cette fois en ce qui concerne le module *q* :

- le résidu modulaire m_2 du message masqué est déterminé par $m_2=(m+\mu_2.q) \bmod (\lambda_2.q)$;

- l'exposant masqué d_2 est calculé par $d_2 = d_q + \tau_2.(q-1)$, où $d_q=d \bmod (q-1)$.

Selon une possibilité de réalisation, on peut choisir les entiers λ_1 et λ_2 de telle sorte que les modules masqués $(\lambda_1.p)$ et $(\lambda_2.q)$ soient des nombres de même longueur, ce qui constitue une solution au problème exposé dans l'article cité en introduction et améliore ainsi la sécurité du procédé.

Une fois les valeurs utilisées dans les calculs d'exponentiation modulaire déterminées aux étapes E8 et E10, on peut procéder à ces calculs, comme détaillé maintenant.

On procède à l'étape E12 à l'exponentiation modulaire du résidu modulaire masqué m_1 au moyen de l'exposant masqué d_1 précédemment déterminé en utilisant comme précédemment le module masqué $(\lambda_1.p)$. Le résultat modulaire masqué S_1 relatif au module p (et calculé ici en utilisant le module masqué $\lambda_1.p$) s'écrit donc selon la formule :

$$S_1 = (m_1)^{d_1} \bmod (\lambda_1.p)$$

On peut noter que, l'entier λ_1 étant un nombre aléatoire, le résultat modulaire masqué S_1 est également aléatoire, ce qui améliore la sécurité.

On procède de manière analogue au calcul du résultat modulaire masqué S_2 à l'étape E14 selon la formule :

$$S_2 = (m_2)^{d_2} \bmod (\lambda_2.q)$$

Cette opération utilise donc le résidu modulaire masqué m_2 et l'exposant masqué d_2 déterminé à l'étape E10, ainsi que le module masqué $(\lambda_2.q)$.

On peut remarquer que les résultats modulaires masqués S_1 et S_2 pourraient être obtenus par d'autres opérations. Par exemple, en combinaison ou non avec la technique de masquage des modules qui vient d'être décrite, les résultats modulaires S_1 et S_2 pourraient être masqués par addition d'un nombre entier (éventuellement déterminé par tirage de nombre aléatoire) de fois le module p ou q associé.

Les résultats modulaires S_1 et S_2 ayant été obtenus comme précisé ci-dessus pour chacun des modules p et q en utilisant les modules masqués

($\lambda_1.p$) et ($\lambda_2.q$), la signature S est obtenue par recombinaison linéaire des résultats modulaires selon une formule type :

$S=[(S_2-S_1).A_{pq} \bmod (q)].p+S_1$, où A_{pq} est l'inverse modulaire de p modulo q défini par $p.A_{pq} = 1 \bmod q$.

La formule de recombinaison est du type qui vient d'être indiqué, mais elle pourrait être différente de la formule donnée ci-dessus ; en effet, en variante, on pourrait par exemple utiliser la formule suivante :

$S=[(S_1-S_2).B_{qp} \bmod (p)].q+S_2$, où B_{qp} est l'inverse modulaire de q modulo p, tel que $q.B_{qp}=1 \bmod p$.

On peut remarquer les formules de recombinaison proposées utilisent les modules p et q de la clé privée, et non les modules masqués.

La signature S ainsi obtenue est strictement égale à la signature qui aurait été obtenue sans masquage (c'est-à-dire que sa valeur est positive ou nulle et strictement inférieure au module public $n=p.q$), et ce bien que les calculs des résidus modulaires et d'exponentiation modulaire aient été effectués en utilisant les modules masqués ($\lambda_1.p$) et ($\lambda_2.p$).

En effet, si deux nombres sont égaux modulo un multiple entier d'un module (par exemple modulo $\lambda_1.p$), ils sont également égaux modulo ce module (ici modulo p), de telle sorte que le résultat modulaire masqué S_1 est égal modulo p au résultat modulaire non masqué s_1 avec $s_1 = (m \bmod p)^{d_p} \bmod p$, de telle sorte que S_1 s'écrit $S_1=s_1+k.p$.

Pour la raison qui vient d'être indiquée, le résultat modulaire masqué S_2 est égal au résultat modulaire non masqué s_2 modulo q (où $s_2 = (m \bmod q)^{d_q} \bmod q$).

Ainsi, si l'on explicite la signature S calculée au moyen des résultats modulaires masqués par la première formule de recombinaison donnée ci-dessus, on obtient :

$S=[(s_2-s_1).A_{pq} \bmod (q)].p-[k.pA_{pq} \bmod (q)].p+s_1+k.p$,

ce qui donne, d'après la définition de A_{pq} donnée ci-dessus :

$S=[(s_2-s_1).A_{pq} \bmod (q)].p+s_1$, ce qui correspond précisément à la recombinaison des résultats modulaires non masqués qui donnent la signature du message.

L'exemple qui vient d'être donné n'est qu'un mode de réalisation possible de l'invention. Comme déjà mentionné, celle-ci s'applique notamment au cas du déchiffrement d'un message m au moyen de la clé privée (d, p, q).

5

REVENDICATIONS

1. Procédé de traitement de données transformant un premier message (m) en un second message (S) au moyen d'une clé privée composée d'un exposant (d) et de deux nombres premiers (p,q), le second message (S) étant le résultat d'une exponentiation modulaire du premier message (m) audit exposant (d) modulo le produit des deux nombres premiers (p,q), caractérisé en ce qu'il comprend les étapes suivantes :

- pour chaque nombre premier (p;q), obtention d'un résultat modulaire (S_1;S_2) incluant une étape d'exponentiation modulaire à un exposant (d_1;d_2) dépendant dudit exposant (d), le résultat modulaire étant masqué pour l'un au moins des deux nombres premiers (p,q) ;

- obtention du second message (S) par recombinaison des résultats modulaires (S_1,S_2).

2. Procédé selon la revendication 1, caractérisé en ce que ladite recombinaison est réalisée par une combinaison d'additions modulaires et de multiplications modulaires.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que ladite recombinaison utilise pour modules les deux nombres premiers (p,q).

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce qu'il comporte, pour chaque nombre premier (p;q), une étape de réduction d'un nombre ($m+\mu_1 p$;$m+\mu_2 q$) dépendant du premier message (m) modulo le produit du nombre premier (p;q) et d'un entier associé (λ_1;λ_2), afin d'obtenir un résidu modulaire (m_1;m_2).

5. Procédé selon la revendication 4, caractérisé en ce qu'il comporte, pour chaque nombre premier (p;q), une étape d'exponentiation modulaire du résidu modulaire (m_1;m_2), à l'exposant (d_1;d_2) dépendant dudit exposant (d),

modulo le produit du nombre premier (p;q) et de l'entier associé ($\lambda_1;\lambda_2$) afin d'obtenir le résultat modulaire ($S_1;S_2$).

6. Procédé selon la revendication 4 ou 5, caractérisé en ce que, pour au moins un nombre premier (p;q), l'entier associé ($\lambda_1;\lambda_2$) est déterminé par tirage de nombres aléatoires.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que la recombinaison des résultats modulaires comprend les étapes suivantes :

- soustraction du résultat modulaire (S_1) obtenu pour un premier nombre premier (p) au résultat modulaire (S_2) obtenu pour le second nombre premier (q) afin d'obtenir une différence (S_2-S_1) ;
- multiplication de la différence (S_2-S_1) par l'inverse modulaire (A_{pq}) du premier nombre premier (p) modulo le second nombre premier (q) afin d'obtenir un produit ;
- réduction du produit modulo le second nombre premier (q) et multiplication du résultat de cette réduction par le premier nombre premier (p) afin d'obtenir une valeur ;
- addition de cette valeur au résultat modulaire (S_1) obtenu pour le premier nombre premier (p) afin d'obtenir le second message (S).

8. Entité électronique permettant la transformation d'un premier message (m) en un second message (S) au moyen d'une clé privée composée d'un exposant (d) et de deux nombres premiers (p,q), le second message (S) étant le résultat d'une exponentiation modulaire du premier message (m) audit exposant (d) modulo le produit des deux nombres premiers (p,q), caractérisé en ce qu'elle comprend :

- des moyens d'obtention, pour chaque nombre premier (p;q), d'un résultat modulaire ($S_1;S_2$) incluant des moyens d'exponentiation modulaire à un exposant ($d_1;d_2$) dépendant dudit exposant (d) et aptes à générer un résultat modulaire masqué pour l'un au moins des deux nombres premiers (p,q) ;

- des moyens d'obtention du second message (S) par recombinaison des résultats modulaires (S_1,S_2).

9. Entité électronique selon la revendication 8, caractérisé en ce que les moyens d'obtention du second message (S) sont aptes à générer ladite recombinaison par une combinaison d'additions modulaires et de multiplications modulaires.

10. Entité électronique selon la revendication 8 ou 9, caractérisé en ce que les moyens d'obtention du second message (S) sont aptes à utiliser pour modules de ladite recombinaison les deux nombres premiers (p,q).

11. Entité électronique selon l'une des revendications 8 à 10, caractérisé en ce qu'elle comporte des moyens pour réduire, pour chaque nombre premier (p;q), un nombre dépendant du premier message (m) modulo le produit du nombre premier (p;q) et d'un entier associé (λ_1;λ_2), afin d'obtenir un résidu modulaire (m_1;m_2).

12. Entité électronique selon la revendication 11, caractérisé en ce qu'elle comporte des moyens aptes à réaliser, pour chaque nombre premier (p;q), une exponentiation modulaire du résidu modulaire (m_1;m_2), à l'exposant dépendant dudit exposant (d), modulo le produit du nombre premier (p;q) et de l'entier associé (λ_1;λ_2), afin d'obtenir le résultat modulaire (S_1; S_2) ;

13. Entité électronique selon la revendication 11 ou 12, caractérisé par des moyens pour déterminer, pour au moins un nombre premier (p;q), l'entier associé (λ_1;λ_2) par tirage de nombres aléatoires.

14. Entité électronique selon l'une des revendications 8 à 13, caractérisé en ce que les moyens d'obtention du second message (S) par recombinaison des résultats modulaires (S_1,S_2) comprend :

- des moyens de soustraction du résultat modulaire (S_1) obtenu pour un premier nombre premier (p) au résultat modulaire (S_2) obtenu pour le second nombre premier (q) afin d'obtenir une différence (S_2-S_1) ;

- des moyens de multiplication de la différence (S_2-S_1) par l'inverse modulaire (A_{pq}) du premier nombre premier (p) modulo le second nombre premier (q) afin d'obtenir un produit ;

- des moyens de réduction du produit modulo le second nombre premier (q) et de multiplication du résultat de cette réduction par le premier nombre premier (p) afin d'obtenir une valeur ;

- des moyens d'addition de cette valeur au résultat modulaire (S_1) obtenu pour le premier nombre premier (p) afin d'obtenir le second message (S).

15. Carte à microcircuit comprenant une entité électronique selon l'une des revendications 8 à 14.

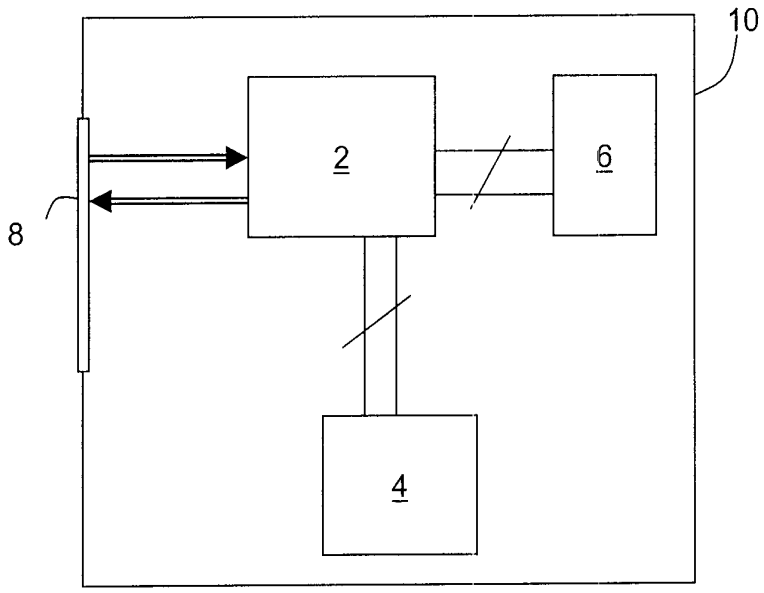


Figure 1

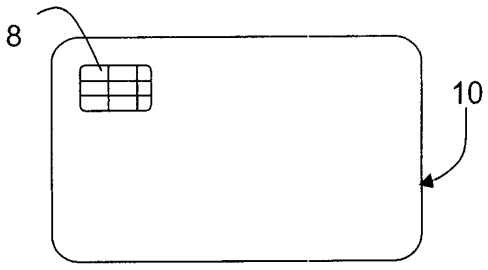


Figure 2

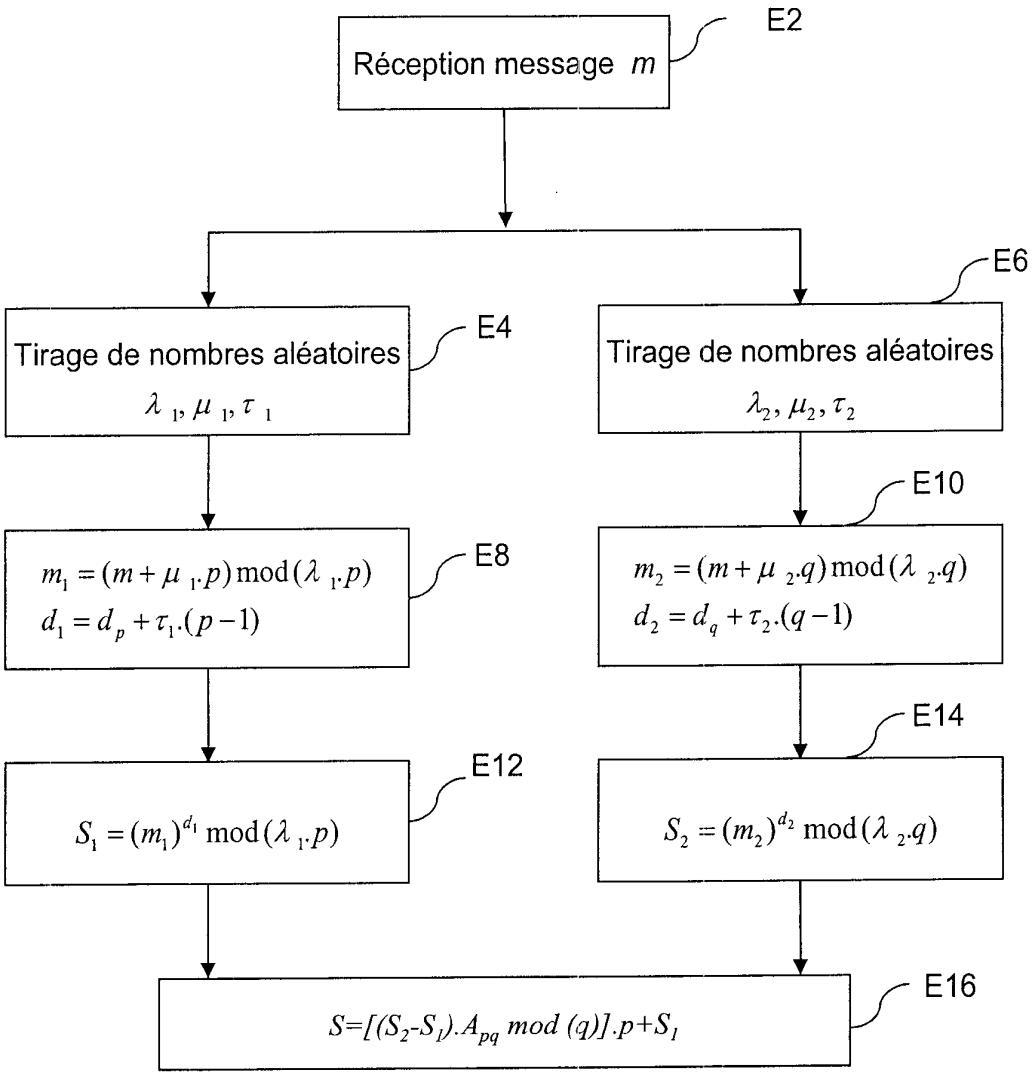

Réception message m
E2
Tirage de nombres aléatoires λ_1, μ_1, τ_1
E4
Tirage de nombres aléatoires λ_2, μ_2, τ_2
E6
$m_1 = (m + \mu_1.p) \bmod (\lambda_1.p)$
$d_1 = d_p + \tau_1.(p-1)$
E8
$m_2 = (m + \mu_2.q) \bmod (\lambda_2.q)$
$d_2 = d_q + \tau_2.(q-1)$
E10
$S_1 = (m_1)^{d_1} \bmod (\lambda_1.p)$
E12
$S_2 = (m_2)^{d_2} \bmod (\lambda_2.q)$
E14
$S=[(S_2-S_1).A_{pq} \bmod (q)].p+S_1$
E16

Figure 3

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 655850
FR 0409766

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	FOUQUE P A ET AL: "Attacking Unbalanced RSA-CRT Using SPA" PROCEEDINGS OF CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2003, 5TH INTERNATIONAL WORKSHOP, COLOGNE, GERMANY, 8 septembre 2003 (2003-09-08), - 10 septembre 2003 (2003-09-10) pages 254-268, XP002321677 BERLIN ISBN: 3-540-40833-9 * partie 5 * * abrégé * -----	1-15	H04L9/06 G06F17/10 G06K19/073
X	BLÖMER J ET AL: "A New CRT-RSA Algorithm Secure Against Bellcore Attacks" PROCEEDINGS OF THE 10TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, CCS 2003, WASHINGTON, DC, USA, 27 octobre 2003 (2003-10-27), - 30 octobre 2003 (2003-10-30) pages 311-320, XP002321676 ISBN: 1-58113-738-9	1-3, 6-10, 13-15	
Y	* partie 4 * * abrégé * -----	4,5,11, 12	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7) G06F
Y	CHEVALLIER-MAMES B: "Self-randomized exponentiation algorithms" LECTURE NOTES IN COMPUTER SCIENCE, SPRINGER VERLAG, NEW YORK, NY, US, vol. 2964, 27 février 2004 (2004-02-27), pages 236-249, XP002297836 ISSN: 0302-9743 * page 2, point 1. * -----	4,5,11, 12	
	-/--		

Date d'achèvement de la recherche	Examinateur
18 mars 2005	Prins, L

CATÉGORIE DES DOCUMENTS CITÉS

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

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

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 655850
FR 0409766

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	QUISQUATER J-J ET AL: "FAST DECIPHERMENT ALGORITHM FOR RSA PUBLIC-KEY CRYPTOSYSTEM" ELECTRONICS LETTERS, IEE STEVENAGE, GB, vol. 18, no. 21, 14 octobre 1982 (1982-10-14), pages 905-907, XP000577331 ISSN: 0013-5194 * page 906, équation (1) * * le document en entier *	7,14	
A	MENEZES A J ET AL: "Handbook of applied cryptography, PASSAGE" HANDBOOK OF APPLIED CRYPTOGRAPHY, CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS, BOCA RATON, FL, CRC PRESS, US, 1997, pages 593,598-629, XP002277222 ISBN: 0-8493-8523-7 * page 613, point 14.75 *	7,14	
A	GROSSSCHADL J: "The Chinese Remainder Theorem and its application in a high-speed RSA crypto chip" COMPUTER SECURITY APPLICATIONS, 2000. ACSAC '00. 16TH ANNUAL CONFERENCE NEW ORLEANS, LA, USA 11-15 DEC. 2000, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 11 décembre 2000 (2000-12-11), pages 384-393, XP010529836 ISBN: 0-7695-0859-6 * partie 1-3 *	1-15	DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

Date d'achèvement de la recherche	Examinateur
18 mars 2005	Prins, L

CATÉGORIE DES DOCUMENTS CITÉS

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

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

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)