(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
20 février 2003 (20.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/014916 A1

(51) Classification internationale des brevets[7] : G06F 7/72

(21) Numéro de la demande internationale :
PCT/FR02/02771

(22) Date de dépôt international : 31 juillet 2002 (31.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01/10671 10 août 2001 (10.08.2001) FR

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

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **JOYE, Marc** [BE/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR). **VILLEGAS, Karine** [FR/FR]; 162, chemin de Lieutaud, F-13420 Gèmenos (FR).

(74) Mandataire : **BRUYERE, Pierre**; Gemplus, BP 100, F-13881 Gèmenos 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*

Publiée :

— *avec rapport de recherche internationale*

[Suite sur la page suivante]

(54) Title: SECURE METHOD FOR PERFORMING A MODULAR EXPONENTIATION OPERATION

(54) Titre : PROCEDE SECURISE DE REALISATION D'UNE OPERATION D'EXPONENTIATION MODULAIRE

(57) Abstract: The invention concerns a secure method for performing an exponentiation operation which consists in carrying out an operation of type U = V^W modulo X. U, V, X are integers, W is an integer used in the form of a number W* masked by a fractional masking parameter randomly selected at each execution of the method. The invention is applicable to smart cards.

(57) Abrégé : L'invention concerne un procédé sécurisé de réalisation d'une opération d'exponentiation au cours duquel on réalise une opération du type U = V^W modulo X. U, V, X sont des nombres entiers, W est un nombre entier utilisé sous la forme d'un nombre W* masqué par un paramètre de masquage fractionnaire choisi de manière aléatoire à chaque exécution du procédé. Application aux cartes à puce.

WO 03/014916 A1

— *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 SECURISE DE REALISATION D'UNE OPERATION D'EXPONENTIATION MODULAIRE

La présente invention concerne un procédé sécurisé pour réaliser une opération d'exponentiation, avec application notamment dans le domaine de la cryptographie. L'invention s'applique en particulier à des algorithmes cryptographiques mis en œuvre dans des dispositifs électroniques tels que des cartes à puce.

De nombreux algorithmes cryptographiques sont basés sur des calculs d'exponentiation du type U = V^W modulo X, où U, V et X sont des nombres entiers le plus souvent de grande taille, et W un nombre prédéterminé. Les nombres U, V peuvent correspondre par exemple à un texte chiffré ou à chiffrer, une donnée signée ou à signer, une donnée vérifiée ou à vérifier, etc. Les nombres W et X peuvent correspondrent à des éléments de clés, privées ou publiques utilisées pour le chiffrage ou le déchiffrage des nombres U, V.

L'un de ces algorithmes est l'algorithme RSA (de Rivest, Shamir et Adleman), qui permet d'obtenir une signature ou un message déchiffré s à partir d'une clé privée comprenant trois nombres entiers d, p et q, p et q étant des nombres premiers de grande taille dont le produit est égal à N. Dans un exemple typique, d et N sont de 1024 bits, et p et q sont de 512 bits.

De nombreux ouvrages présentent en détails l'algorithme RSA, il est cependant nécessaire de rappeler ici les principes de base de cet algorithme, qui permet de calculer la signature s :

$$s = m^d \bmod (p.q) = m^d \bmod (N)$$

L'algorithme RSA peut être mis en oeuvre en utilisant le théorème des restes chinois (en anglais Chinese Remainder Theorem). Par l'application de ce théorème, la signature s est obtenue par :

$s = m^d \bmod(N) = CRT(s_p, s_q)$

La fonction $CRT(s_p, s_q)$ est couramment appelée formule de recombinaison selon le théorème des restes chinois. La fonction CRT se calcule par exemple de la manière suivante :

$CRT(s_p, s_q) = s_p + p \times Y$, avec :

$Y = i_p(s_q - s_p) \bmod(q)$

$d_p = d \bmod(p-1)$, $s_p = m^{d_p} \bmod(p)$

$d_q = d \bmod(q-1)$, $s_q = m^{d_q} \bmod(q)$

$i_p = (1/p) \bmod(q)$

Le même algorithme permet de vérifier la validité de la signature s d'un message m en vérifiant que la relation :

$m = s^e \bmod(N)$

est satisfaite.

Les nombres e et N forment la clé publique associée à la clé privée (d, p, q) ; les nombres e et N vérifient les relations :

$N = p \times q$

$pgcd(e, \Phi(N)) = 1$

$e \times d = 1 \bmod(\Phi(N))$,

$\Phi(N)$ étant la fonction indicatrice d'Euler définie par $\Phi(N) = (p-1)(q-1)$.

On notera que tous les éléments d, p, q d'une clé privée et tous les éléments e, N d'une clé publique associée sont impairs. En effet p et q étant des grands nombres premiers, ils sont nécessairement impairs. $\Phi(N) = (p-1)(q-1)$ est donc pair et $N = p \times q$ est impair. Comme e et $\Phi(N)$ sont premiers entre eux, e est impair. Comme $e \times d = 1 \bmod(\Phi(N))$, $e \times d$ est impair, et donc d est également impair.

D'autres algorithmes, cryptographiques ou non, utilisent également des opérations d'exponentiation de type $U = V^W$ modulo X, éventuellement mis en œuvre par la théorème des restes chinois. Par exemple le cryptosystème

de Rabin-Williams ou encore l'échange de clé Diffie-Hellman modulo un nombre composé.

Un utilisateur malveillant peut éventuellement engager des attaques à canaux cachés, visant à découvrir notamment des informations confidentielles (comme par exemple les nombres d ou p) contenues et manipulées dans des traitements effectués par le dispositif de calcul exécutant une opération d'exponentiation. Les attaques à canaux cachés les plus connues sont dites simples ou différentielles. On entend par attaque à canal caché simple ou différentielle, une attaque basée sur une grandeur physique mesurable de l'extérieur du dispositif, et dont l'analyse directe (attaque simple) ou l'analyse selon une méthode statistique (attaque différentielle) permet de découvrir des informations contenues et manipulées dans des traitements réalisés dans le dispositif. Ces attaques peuvent ainsi permettre de découvrir des informations confidentielles. Ces attaques ont notamment été dévoilées par Paul Kocher (Advances in Cryptology - CRYPTO'99, vol. 1666 of Lecture Notes in Computer Science, pp.388-397. Springer-Verlag, 1999).

Parmi les grandeurs physiques qui peuvent être exploitées à ces fins, on peut citer le temps d'exécution, la consommation en courant, le champ électromagnétique rayonné par la partie du composant utilisée pour exécuter le calcul, etc. Ces attaques sont basées sur le fait que, au cours de l'exécution d'un algorithme, la manipulation d'un bit, c'est à dire son traitement par une instruction particulière, laisse une empreinte particulière sur la grandeur physique considérée, selon la valeur de ce bit et / ou selon l'instruction.

Les algorithmes d'exponentiation précités ont dû inclure des contre-mesures pour empêcher de telles attaques d'aboutir.

Paul Kocher a notamment proposé, dans le document WO 99/35782, une méthode qui consiste notamment à masquer les variables dérivées d_p, d_q du nombre d par l'ajout d'un nombre entier aléatoire. Plus précisément, les variables d_p, d_q ne sont pas utilisées directement dans l'algorithme, mais elles sont utilisées sous la forme de nombres masqués $d_i^* = d_i + r_i \times (p-1)$, avec i égal à p ou q et r_i (r_p ou r_q) des nombres entiers aléatoires, modifiés à chaque mise en œuvre de l'algorithme. Dans un exemple dévoilé dans le document WO 99/35782, cette méthode est utilisée dans le cadre d'un algorithme RSA mis en œuvre selon le théorème des restes chinois. L'algorithme se décompose alors de la manière suivante :

On calcule tout d'abord s_p^* et s_q^* :

$$s_p^* = [m^{d_p^*}] \bmod(p) = [m^{(d_p + r_p \times (p-1))}] \bmod(p)$$

$$s_q^* = [m^{d_q^*}] \bmod(q) = [m^{(d_q + r_q \times (p-1))}] \bmod(q)$$

On calcule ensuite le nombre s par la formule de recombinaison :

$$s = s^* = CRT(s_p^*, s_q^*).$$

L'égalité $s = s^*$ se déduit de la définition de d_p, d_q, d_p^*, d_q^* et du théorème de Fermat, selon lequel $A^{(B-1)} = 1 \bmod(B)$ lorsque B est un nombre entier premier et que A est relativement premier avec B. Dans le cas présent, on déduit du théorème de Fermat :

$$m^{d_p^*} = m^{(d_p + r_p \times (p-1))}$$

$$= m^{d_p} \times m^{(r_p \times (p-1))} = m^{d_p} \times 1 [\bmod(p)].$$

Puisque $m^{d_p^*} = [m^{d_p}] [\bmod(p)]$, on a $s_p = s_p^*$. Un raisonnement similaire permet de déduire $s_q = s_q^*$. Finalement, comme $s_p = s_p^*$ et $s_q = s_q^*$, $s = s^*$.

La méthode dévoilée dans le document WO 99/35782 est notamment efficace pour contrer les attaques à canaux cachés différentielles, elle complique également les attaques simples.

Cependant, cette méthode n'est pas efficace contre une attaque particulière détaillée ci dessous (que l'on appellera par la suite par souci de simplification

attaque CRT) dans le cadre d'un exemple relatif à l'algorithme RSA. Plus généralement, l'attaque CRT peut être envisagée pour tout algorithme mis en œuvre par l'intermédiaire du théorème des restes chinois.

Dans l'exemple d'un algorithme RSA mis en œuvre à l'aide du théorème des restes chinois, l'attaque CRT permet d'obtenir le nombre p de la clé privée. On a vu précédemment que la formule de recombinaison permettant de calculer s s'écrit :

$$s = CRT(s_p, s_q) = s_p + p \times Y, \text{ avec}$$
$$Y = i_p \times (s_q - s_p) \bmod (q)$$

Si p, q sont de a bits (par exemple 512 bits), alors, i_p, s_p, s_q sont de a bits, de même que Y. Le produit pxY et le nombre s sont donc de 2a bits. Comme s_p est de a bits, on en déduit que les a bits de poids fort de s sont égaux aux a bits de poids fort du produit pxY.

Par ailleurs, le poids de Hamming H(Y) du nombre Y peut être obtenu par une attaque à canal caché simple lors du calcul de Y. On rappelle que le poids de Hamming du nombre Y est le nombre de bits à "1" du nombre Y.

Connaissant les bits de poids forts du produit pxY et le poids de Hamming du nombre Y, il est possible de retrouver le nombre p par itérations successives de la manière suivante :

- on fait une hypothèse sur la valeur de b bits (par exemple b = 8) de poids le plus fort de p et on détermine les b bits du poids fort correspondant de Y à partir des bits de poids fort du produit pxY, lesquels sont donnés par la valeur de s. On calcule ensuite la probabilité pour que l'hypothèse sur les b bits de poids le plus fort de p soit correcte à partir du poids de Hamming de Y, mesuré par un canal caché.

- on réitère pour chaque valeur possible des b bits de poids les plus forts de p et on retient finalement l'hypothèse la plus probable pour ces b bits.

- on réitère ensuite pour chaque paquet de b bits de p, jusqu'à l'obtention d'un nombre suffisant des bits de p.

La méthode dévoilée dans le document WO 99/35782 n'est pas efficace contre cette attaque CRT. En effet, dans le document WO 99/35782, la formule de recombinaison utilisée s'écrit :

$$s = CRT(s_p^*, s_q^*) = s_p^* + p \times Y^*,$$

avec s, $p \times Y^*$ de taille 2a bits et s_p^* de taille a bits.

Il est donc possible, par une attaque CRT telle qu'on vient de la décrire, de déterminer le nombre p à partir du nombre s connu, du produit $p \times Y^*$, et du poids de Hamming de (Y^*).

Au vu des limites de la méthode dévoilée dans le document WO 99/35782, un objet de l'invention est de proposer un procédé sécurisé de réalisation d'une opération d'exponentiation, protégé contre toutes les attaques, y compris les attaques CRT telles que décrites ci-dessus.

Un autre objet de l'invention est de proposer un procédé sécurisé de réalisation d'une opération d'exponentiation, au moins aussi performant que le procédé dévoilé dans le document WO 99/35782, notamment en terme de taille de circuit et de temps de calcul.

Un autre objet de l'invention enfin est de réaliser un procédé sécurisé de calcul d'une opération d'exponentiation, pouvant être incorporé à tout procédé de calcul au cours duquel un calcul du type $U = V^W$ modulo X doit être réalisé.

Avec ces objectifs en vue, l'invention a pour objet un procédé sécurisé de réalisation d'une opération d'exponentiation au cours duquel on réalise une opération du type $U = V^W$ modulo X, U, V, X étant des nombres

entiers, W étant un nombre entier utilisé sous la forme d'un nombre W* masqué par un paramètre de masquage choisi de manière aléatoire à chaque exécution du procédé.

Selon l'invention, le paramètre de masquage est un nombre fractionnaire.

Les nombres W, X sont en pratique des nombres qui doivent être maintenus cachés, comme des éléments d'une clé privée, et / ou des nombres dérivés d'une telle clé. Par exemple, si le procédé selon l'invention est utilisé dans le cadre d'un algorithme RSA mis en œuvre selon le théorème des restes chinois, le nombre W peut être les variables d_p, d_q utilisées de manière habituelle. La taille des nombres W, X est indifférente, elle est par exemple de 1024 bits.

L'utilisation d'un paramètre de masquage aléatoire fractionnaire, au lieu d'un paramètre de masquage aléatoire entier, rend impossible l'obtention d'une information sur le nombre W par un attaque à canaux cachés, ou par une attaque CRT, comme on le verra mieux par la suite dans des exemples.

Selon des modes de réalisation préférés, le paramètre de masquage est de la forme R/K. R est un nombre entier aléatoire modifié à chaque exécution du procédé. La taille du nombre R détermine la sécurité de l'algorithme par rapport aux attaques dites différentielles, R peut être choisi par exemple de taille 32 bits. K est un nombre entier diviseur du nombre $\Phi(X)$, Φ étant la fonction indicatrice d'Euler. K peut être choisi constant ou bien peut être modifié à chaque exécution du procédé. La taille de K est indifférente, elle est par exemple proche de la taille du nombre R.

Avantageusement, le nombre masqué W* est de la forme $W^* = \overline{W} + \overline{R}$. $\overline{W}$ est la partie par défaut du résultat de la division de W par K, et $\overline{R}$ est égal au produit du paramètre de masquage (R/K) par le nombre $\Phi(X)$.

Le résultat U peut alors être exprimé en fonction de (U*)^K modulo X, avec U* = V^W* modulo X.

Plus précisément, le résultat U est égal à U = (U*)^K × V^Z modulo X, avec U* = V^W* modulo X. Z est le reste de la division entière de W par K.

Le procédé de l'invention, tel que décrit ci-dessus peut être utilisé avantageusement dans un procédé cryptographique global.

Dans un exemple qui sera décrit plus précisément, le procédé cryptographique est de type RSA, et il est mis en œuvre selon le théorème des restes chinois. Dans ce cas, l'invention est utilisée notamment pour masquer une clé éventuellement dérivée (par exemple les clés dérivées d_p, d_q) par un paramètre de masquage choisi de manière aléatoire à chaque exécution du procédé, le paramètre de masquage étant un nombre fractionnaire.

L'invention a également pour objet un composant électronique comprenant un circuit de calcul pour mettre en œuvre un procédé selon l'invention, par exemple, mais non nécessairement, dans le cadre d'un algorithme cryptographique .

Enfin, l'invention a également pour objet une carte à puce comprenant ledit composant électronique.

L'invention et les avantages qui en découlent apparaîtront plus clairement à la lecture de la description qui suit d'un exemple particulier de réalisation de l'invention, donné à titre purement indicatif et en référence à la figure unique en annexe. Celle-ci est un dispositif électronique permettant de mettre en œuvre l'invention.

La figure unique représente sous forme de schéma bloc un dispositif 1 électronique apte à réaliser des calculs d'exponentiation. Dans l'exemple, ce dispositif est une carte à puce destinée à exécuter un programme

cryptographique. A cette fin, le dispositif 1 réunit dans une puce des moyens de calcul programmés, composés d'une unité centrale 2 reliée fonctionnellement à un ensemble de mémoires dont :

- une mémoire 4 accessible en lecture seulement, dans l'exemple du type ROM masque, aussi connue sous l'appellation anglaise "mask read-only memory (mask ROM)",
- une mémoire 6 re-programmable électriquement, dans l'exemple du type EEPROM (de l'anglais "electrically erasable programmable ROM"), et
- une mémoire de travail 8 accessible en lecture et en écriture, dans l'exemple du type RAM (de l'anglais "random access memory"). Cette mémoire comprend notamment les registres utilisés par le dispositif 1.

Le code exécutable correspondant à l'algorithme d'exponentiation est contenu en mémoire programme. Ce code peut en pratique être contenu en mémoire 4, accessible en lecture seulement, et/ou en mémoire 6, réinscriptible.

L'unité centrale 2 est reliée à une interface de communication 10 qui assure l'échange de signaux vis-à-vis de l'extérieur et l'alimentation de la puce. Cette interface peut comprendre des plots sur la carte pour une connexion dite "à contact" avec un lecteur, et/ou une antenne dans le cas d'une carte dite "sans contact".

L'une des fonctions du dispositif 1 est de crypter ou décrypter un message m confidentiel respectivement transmis vers, ou reçu de, l'extérieur. Ce message peut concerner par exemple des codes personnels, des informations médicales, une comptabilité sur des transactions bancaires ou commerciales, des autorisations d'accès à certains services restreints, etc. Une autre fonction est de calculer ou de vérifier une signature numérique.

A cette fin, l'unité centrale 2 exécute un algorithme cryptographique, utilisant un calcul d'exponentiation, sur des données de programmation qui sont stockées dans les parties ROM masque 4 et/ou EEPROM 6.

Dans l'exemple décrit ici, l'algorithme d'exponentiation est de type RSA, mis en oeuvre par l'utilisation du théorème des restes chinois. L'algorithme est utilisé pour signer un message m à partir d'une clé privée comprenant trois nombres entiers d, p et q. Dans l'exemple, d est de 1024 bits, et p et q sont de 512 bits.

Dans l'exemple, on réalise un calcul d'exponentiation $s = m^d \bmod(p.q)$, où m est un message prédéterminé et d, p, q des nombres entiers éléments de la clé privée. Le nombre s obtenu constitue une signature du message m.

Les nombres d, p, q (éléments de la clé) sont stockés dans une portion de la mémoire re-inscriptible 6, de type EEPROM dans l'exemple.

Lorsque le dispositif 1 de calcul d'exponentiation est sollicité pour le calcul d'exponentiation, l'unité centrale mémorise tout d'abord le nombre m, transmis par l'interface de communication 10, en mémoire de travail 8, dans un registre de calcul. L'unité centrale va ensuite lire les clés d, p, q contenues en mémoire re-inscriptible 6, pour les mémoriser temporairement, le temps du calcul d'exponentiation, dans un registre de calcul de la mémoire de travail 8. L'unité centrale lance alors l'algorithme d'exponentiation.

Selon l'invention, les clés dérivées d_p, d_q de la clé d sont masquées par un nombre fractionnaire aléatoire de la manière suivante.

L'unité centrale choisit tout d'abord un nombre k_p diviseur de p-1, et un nombre k_q diviseur de q-1, p, q étant des éléments de la clé ; k_p, k_q sont mémorisés dans

un autre registre de calcul de la mémoire de travail 8. Selon le mode de réalisation choisi, k_p peut être modifié à chaque mis en œuvre de l'algorithme ou bien peut être maintenu constant. La taille de k_p est indifférente, mais nécessairement inférieure à la taille de p-1.

L'unité centrale choisit également deux nombres r_p, r_q, aléatoires et les mémorise dans deux autres registres de calcul de la mémoire de travail. r_p, r_q sont de préférence modifiés à chaque mise en œuvre de l'algorithme. La taille des nombres r_p, r_q est généralement un compromis entre d'une part la taille de la mémoire 8 dans laquelle ils sont mémorisés et les temps de calcul (qui augmentent avec la taille des nombres r_p, r_q) et d'autre part la sécurité de l'algorithme (qui augmente également avec la taille des nombres r_p, r_q).

L'unité centrale calcule ensuite les variables d_p^*, a_p, d_q^*, a_q suivantes :

$$d_p^* = \bar{d}_p + \bar{r}_p, \qquad \text{(formule 1)}$$

$$a_p = d_p \bmod k_p \qquad \text{(formule 2)}$$

avec $\bar{d}_p = \lfloor d_p / k_p \rfloor$ et $\bar{r}_p = r_p \times (p-1)/k_p$

$$d_q^* = \bar{d}_q + \bar{r}_q, \qquad \text{(formule 3)}$$

$$a_q = d_q \bmod k_q \qquad \text{(formule 4)}$$

avec $\bar{d}_q = \lfloor d_q / k_q \rfloor$ et $\bar{r}_q = r_q \times (q-1)/k_q$

$\bar{d}_p$, a_p sont respectivement le résultat et le reste de la division entière de d_p par k_p

$\bar{d}_q$, a_q sont respectivement le résultat et le reste de la division entière de d_q par k_q

L'unité centrale mémorise les variables d_p^*, a_p, d_q^*, a_q dans des registres de la mémoire de travail. Par la suite, les variables intermédiaires obtenues tout au long du calcul seront également mémorisées dans une portion de la mémoire de travail 8.

L'unité centrale calcule ensuite les variables :

$$s_p^* = m^{d_p^*} \bmod p$$

$$s_q^* = m^{d_q^*} \bmod q$$

puis la signature s à partir des variables s_p*, a_p, k_p, s_q*, a_q, k_q. Pour cela, l'unité centrale utilise le fait que :

$$s_p = [(m^{d_p}*)^{k_p} \times m^{a_p}] \bmod(p), \quad \text{(formule 5)}$$

$$s_q = [(m^{d_q}*)^{k_q} \times m^{a_q}] \bmod(q), \quad \text{(formule 6)}$$

$$s = CRT(s_p, s_q) \quad \text{(formule 7)}$$

On notera que les expressions ci-dessus de s_p, s_q se déduisent du fait que $\bar{d}_p$, $\bar{d}_q$ et a_p, a_q sont définis de sorte que $d_p = \bar{d}_p \times k_p + a_p$ et $d_p = \bar{d}_p \times k_p + a_p$, ce qui permet d'écrire :

$$\begin{aligned} s_p &= [m^{d_p}] \bmod(p) \\ &= (m^{\bar{d}_p})^{k_p} \times m^{a_p} \bmod(p) \\ &= m^{(\bar{d}_p \times k_p)} \times m^{a_p} \bmod(p) \\ &= m^{(\bar{d}_p \times k_p)} \times m^{(r_p \times (p-1))} \times m^{a_p} \bmod(p) \\ &\qquad \text{(th. de Fermat)} \\ &= m^{[(\bar{d}_p + \bar{r}_p) \times k_p]} \times m^{a_p} \bmod(p) \\ &= (m^{d_p}*)^{k_p} \times m^{a_p} \bmod(p) \\ &= (s_p*)^{k_p} \times m^{a_p} \bmod(p). \end{aligned}$$

La démonstration de l'exactitude de l'expression pour s_q est bien entendu similaire.

Dans un exemple de mise en œuvre pratique où $k_p = k_q$ et $a_p = a_q$, les égalités 5 et 6 permettent de simplifier l'égalité 7 sous la forme :

$$\begin{aligned} s = CRT(s_p, s_q) &= \{[CRT(s_p*, s_q*)]^{k_p} \times m^{a_p}\} \bmod N \\ &= \{(s_p* + p \times Y*)^{k_p} \times m^{a_p}\} \bmod N \quad \text{(formule 7')} \\ &= \{[CRT(s_p*, s_q*)]^{k_p} \times m^{a_p}\} \bmod N \end{aligned}$$

Dans un exemple numérique, on choisit $k_p = k_q = 2$. Dans ce cas, $a_p = a_q = 1$ car tous les éléments d'une clé secrète et d'une clé publique associée sont impairs (voir plus haut). En effet, d, p et q étant des nombres impairs, les nombres $d_p = d \bmod(p-1)$ et $d_q = q \bmod(q-1)$ sont également impairs. En conséquence, a_p, le reste de la division de d_p par $k_p = 2$ est nécessairement égal à 1. Pour les mêmes raisons, a_q, le reste de la division de d_q par $k_q = 2$ est bien sûr égal à 1.

L'égalité 7 est insensible aux attaques à canaux cachés différentielles et simples. En effet, les termes aléatoires dans les nombres s_p*, s_q* masquent les données d_p, d_q, de même que dans le document WO 99/35782.

Par ailleurs, l'égalité 7 est insensible aux attaques CRT. Ceci apparaît plus clairement sur la formule simplifiée 7'. La somme s_p*+p×Y*, indispensable pour mener à bien une attaque CRT, n'apparaît pas directement dans la relation 7', elle apparaît uniquement à la puissance k_p. Or, il est conjecturé impossible d'extraire de s une racine $k_p^{-ième}$ sans connaître le module N. Il n'est donc pas possible de calculer s_p*+p×Y*, il n'est donc pas possible d'obtenir les bits de p par une attaque CRT.

Un algorithme selon l'invention est donc bien protégé contre toutes ces attaques.

REVENDICATIONS

1. Procédé sécurisé de réalisation d'une opération d'exponentiation au cours duquel on réalise une opération du type U = V^W modulo X, U, V, X étant des nombres entiers, W étant un nombre entier utilisé sous la forme d'un nombre W* masqué par un paramètre de masquage choisi de manière aléatoire à chaque exécution du procédé, caractérisé en ce que le paramètre de masquage est un nombre fractionnaire.

2. Procédé selon la revendication 1, caractérisé en ce que le paramètre de masquage est de la forme R/K, où R est un nombre entier aléatoire et où K est un nombre entier diviseur du nombre $\Phi(X)$, Φ étant une fonction indicatrice d'Euler.

3. Procédé selon la revendication 2, caractérisé en ce que le nombre K et / ou le nombre R sont modifiés à chaque exécution du procédé.

4. Procédé selon la revendication 2 ou la revendication 3, caractérisé en ce que le nombre masqué W* est de la forme $W^* = \overline{W} + \overline{R}$, $\overline{W}$ étant la partie par défaut du résultat de la division de W par K, et $\overline{R}$ étant égal au produit du paramètre de masquage R/K par le nombre $\Phi(X)$.

5. Procédé selon l'une des revendications 2 à 4, caractérisé en ce que le résultat U est fonction de (U*)^K modulo X, avec U* = V^W* modulo X.

6. Utilisation d'un procédé sécurisé selon l'une des revendications 1 à 5 dans un procédé cryptographique.

7. Utilisation d'un procédé sécurisé selon l'une des revendications 1 à 5 dans un procédé cryptographique mis en œuvre selon le théorème des restes chinois, pour masquer une clé éventuellement dérivée par un paramètre de masquage choisi de manière aléatoire à chaque exécution du procédé, le paramètre de masquage étant un nombre fractionnaire.

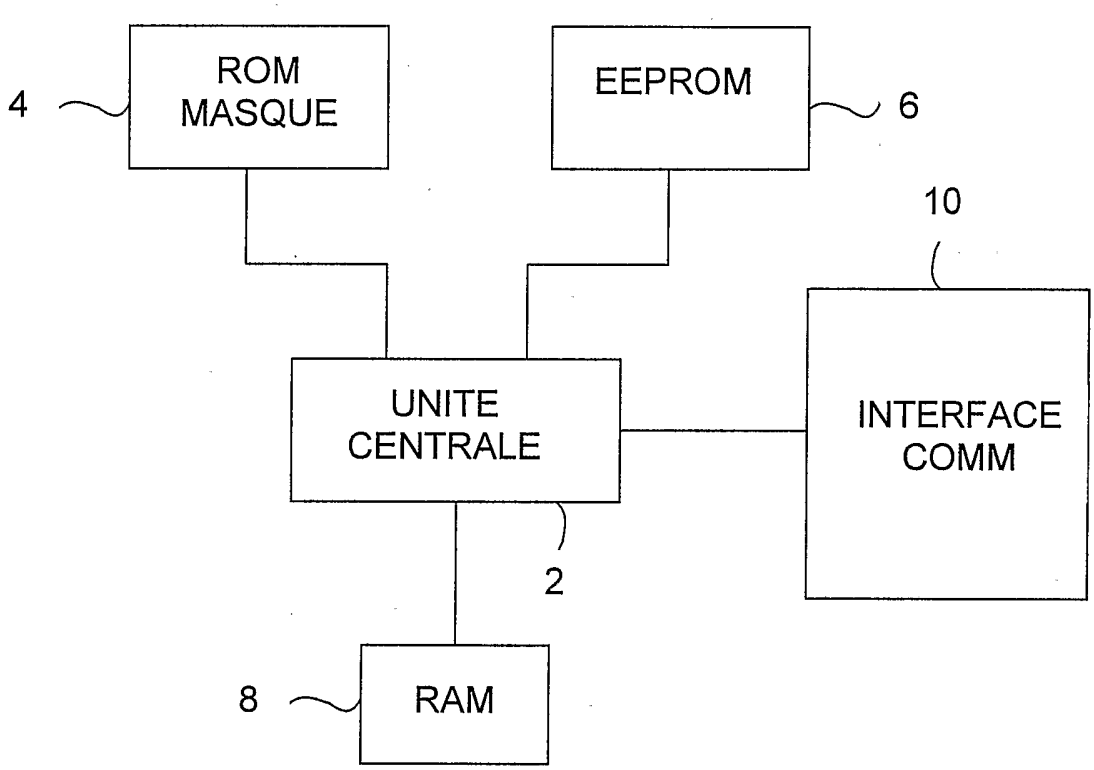
8. Utilisation d'un procédé sécurisé selon la revendication 7, caractérisée en ce que le procédé cryptographique est un procédé de type RSA.

9. Composant électronique comprenant un circuit de calcul pour mettre en œuvre un procédé selon l'une des revendications 1 à 5.

10. Composant électronique comprenant des moyens de mise en œuvre d'un procédé cryptographique utilisant un procédé selon l'une des revendications 1 à 6.

11. Carte à puce comprenant un composant électronique selon la revendication 9 ou la revendication 10.

1/1


ROM
MASQUE
4
EEPROM
6
10
UNITE
CENTRALE
INTERFACE
COMM
2
8
RAM
1

INTERNATIONAL SEARCH REPORT

Inte ›nal Application No
PCT/FR 02/02771

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F7/72

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 G06F

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)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 48974 A (DREXLER HERMANN ;VATER HARALD (DE); GIESECKE & DEVRIENT GMBH (DE)) 5 July 2001 (2001-07-05) claims 13,14; figure	1,7-11
A	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 November 1998 (1998-11-19) figures	1-3,7
A	MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, August 1999 (1999-08), pages 144-157, XP000952221 page 155, paragraph 3 -page 156, paragraph 4	1,2

☐ 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
11 December 2002	23/12/2002

Name and mailing address of the ISA	Authorized officer
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	Verhoof, P

INTERNATIONAL SEARCH REPORT

Inte nal Application No
PCT/FR 02/02771

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0148974 A	05-07-2001	DE 19963408 A1	30-08-2001
		AU 2675401 A	09-07-2001
		WO 0148974 A1	05-07-2001
		EP 1262037 A1	04-12-2002
WO 9852319 A	19-11-1998	US 5991415 A	23-11-1999
		AU 7568598 A	08-12-1998
		EP 0986873 A1	22-03-2000
		WO 9852319 A1	19-11-1998

RAPPORT DE RECHERCHE INTERNATIONALE

Den Internationale No
PCT/FR 02/02771

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

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 G06F

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)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 01 48974 A (DREXLER HERMANN ;VATER HARALD (DE); GIESECKE & DEVRIENT GMBH (DE)) 5 juillet 2001 (2001-07-05) revendications 13,14; figure	1,7-11
A	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 novembre 1998 (1998-11-19) figures	1-3,7
A	MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. INTERNATIONAL WORKSHOP, XX, XX, août 1999 (1999-08), pages 144-157, XP000952221 page 155, alinéa 3 -page 156, alinéa 4	1,2

☐ 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
11 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	Verhoof, P

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 02/02771

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0148974	A	05-07-2001	DE	19963408 A1	30-08-2001
			AU	2675401 A	09-07-2001
			WO	0148974 A1	05-07-2001
			EP	1262037 A1	04-12-2002
WO 9852319	A	19-11-1998	US	5991415 A	23-11-1999
			AU	7568598 A	08-12-1998
			EP	0986873 A1	22-03-2000
			WO	9852319 A1	19-11-1998