(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 807 246**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 03919**

(51) Int Cl[7] : **H 04 L 9/30**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 28.03.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 05.10.01 Bulletin 01/40.

(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) :** *GEMPLUS Société en commandite par actions* — FR.

(72) **Inventeur(s) :** PAILLIER PASCAL.

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

(74) **Mandataire(s) :**

(54) PROCEDE DE GENERATION DE CLES ELECTRONIQUES A PARTIR DE NOMBRES ENTIERS PREMIERS ENTRE EUX ET DISPOSITIF DE MISE EN OEUVRE DU PROCEDE.

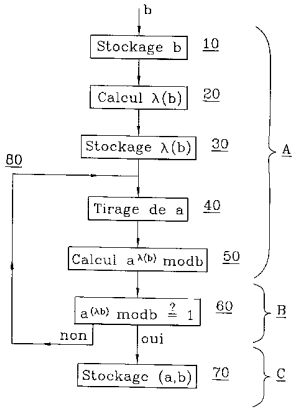
(57) L'invention concerne un procédé de génération de clés électroniques à partir de deux nombres entiers a, b, le procédé comprenant une étape de vérification de la co-primalité desdits nombres a, b. Selon l'invention cette étape de vérification comprend les opérations suivantes:

A) - calcul de l'exponentiation, modulaire $a^{\lambda(b)}$ modb, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

C) - on retient le couple a, b lorsque l'égalité est vérifiée et on réitère avec un autre couple dans le cas contraire.

L'invention s'applique aux cartes à puces à microprocesseur possédant un processeur arithmétique.



FR 2 807 246 - A1

2807246

PROCEDE DE GENERATION DE CLES ELECTRONIQUES A PARTIR DE NOMBRES ENTIERS PREMIERS ENTRE EUX ET DISPOSITIF DE MISE EN ŒUVRE DU PROCEDE.

L'invention concerne un procédé de génération de clés électroniques à partir de nombres entiers premiers entre eux et un dispositif de mise en œuvre du procédé.

L'invention s'applique tout particulièrement à des protocoles de cryptographie à clé publique utilisés pour le cryptage d'informations et/ou l'authentification entre deux entités et/ou la signature électronique de messages.

Elle s'applique en particulier à des protocoles de cryptographie à clé publique tels que le protocole RSA (Rivest Shamir et Adelman), El Gamal, Schnorr, Fiat Shamir.

Dans le cas de telles applications on fait, en effet appel à la génération de grands nombres entiers (pouvant être par exemple être supérieurs ou égaux à 512 bits) pour former une ou plusieurs clés du protocole. Une condition est imposée pour le choix de ces nombres afin qu'ils restent secrets c'est qu'ils doivent être co-premiers ou premiers entre eux.

De façon pratique, le dispositif électronique qui désire générer de tels nombres en vue par exemple de mettre en œuvre un protocole de cryptographie, opère de manière connue de la façon suivante :

-Prendre un nombre entier a (choisi parmi un ensemble de nombres entiers prédéterminés, ou tiré aléatoirement),

-Tirer de façon aléatoire un deuxième nombre entier b,

-Effectuer une opération de vérification de la co-primalité entre les nombres a et b. Cette opération permet de vérifier que les deux nombres entiers a, b obtenus sont premiers entre eux. Elle est réalisée par l'unité centrale du dispositif. L'unité centrale calcule pour cela le plus grand commun diviseur (pgcd) entre ces deux nombres et vérifie que le résultat est égal à 1. En effet on rappelle que deux nombres sont co-premiers si et seulement si leur plus grand commun diviseur est égal à 1.

Il existe pour cela plusieurs techniques bien connues d'implémentation du calcul du pgcd de deux nombres à l'aide d'un microprocesseur.

On peut citer à titre d'exemple les techniques telles que celle du « Binary GCD », du « Extended GCD » ou la technique de Lehmer. Malgré une complexité asymptotique excellente (c'est-à-dire pour des nombres de taille extrêmement grande), ces techniques s'avèrent à la fois difficile à programmer sur des dispositifs portables de type carte à microprocesseur (car complexes) et de performances médiocres pour des nombres de grandes de tailles usuelles (512 bits) qui tendent à ce jour à devenir supérieures à savoir 1024 bits et plus.

L'invention a pour but de remédier à cet inconvénient. Elle a plus particulièrement pour objet un procédé de génération de clés électroniques à partir de deux nombres entiers a, b, le procédé comprenant une étape de vérification de la co-primalité desdits nombres a, b, principalement caractérisé en ce que cette étape de vérification comprend les opérations suivantes :

A) - calcul de l'exponentiation, modulaire $a^{\lambda(b)} \mathrm{mod} b$, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

C) - on retient le couple a, b lorsque l'égalité est vérifiée et on réitère avec un autre couple dans le cas contraire.

Selon une autre caractéristique :

- on choisit un nombre entier b d'une longueur donnée et on le mémorise,
- on tire au hasard un nombre entier a,
- on calcule $a^{\lambda(b)}$modb
- on vérifie que $a^{\lambda(b)} = 1$ modb (ou $a^{\lambda(b)}$modb = 1),
- on mémorise le nombre a dans le cas où l'égalité est vérifiée,
- on réitère les étapes précédentes avec un autre nombre a dans le cas contraire.

Selon une autre caractéristique, dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

L'invention s'applique aux procédés de génération de clés cryptographiques RSA ou El Gamal ou Schnorr.

L'invention a également pour objet un dispositif électronique portable comprenant un processeur arithmétique et une mémoire de programme associée, apte à effectuer des exponentiations modulaires, principalement caractérisé en ce qu'il comprend un programme de vérification de co-primalité de nombres entiers de longueur donnée qui effectue les opérations suivantes :

A) - calcul de l'exponentiation modulaire $a^{\lambda(b)}$modb, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

C) le processeur arithmétique stocke le couple a, b lorsque l'égalité est vérifiée et réitère avec un autre couple dans le cas contraire.

Selon une autre caractéristique, dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

Avantageusement le dispositif électronique portable, est constitué par une carte à puce à microprocesseur.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est faite ci-après et qui est donnée à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

- la figure 1, représente le schéma de principe d'un dispositif électronique portable tel qu'une carte à puce mettant en œuvre le procédé selon l'invention,
- la figure 2, représente le schéma d'un exemple de réalisation de le mise en œuvre du procédé selon l'invention.

Dans la description qui va suivre, on a pris comme exemple de dispositif électronique portable celui des cartes à puces à microprocesseur et on parlera pour simplifier de cartes à microprocesseur.

Dans le cas de la mise en œuvre de protocoles de cryptographie tels que le RSA par exemple, il est comme on la dit nécessaire de déterminer un couple de nombres entiers de longueur donnée, premiers entre eux servant à la génération de clés électroniques du protocole.

Afin de s'assurer que les nombres générés sont premiers entre eux une étape de vérification de coprimalité est réalisée par la carte à microprocesseur

qui met en œuvre le procédé de génération de clés pour le protocole de cryptographie.

En pratique dans le protocole RSA, les deux nombres entiers a, b, restent secrets, ils doivent être premiers entre eux et ont une longueur fixée généralement de 512 bits ou 1024 bits chacun. Selon ce même exemple, un des deux nombres b est un nombre entier choisi à l'avance et stocké parmi un ensemble de nombres générés par la carte à microprocesseur tandis que l'autre nombre a est généré de manière aléatoire par la carte à microprocesseur à l'exécution du protocole. A cette fin, la carte à microprocesseur possède un générateur de nombres aléatoires, capable de fournir un nombre entier de la taille désirée.

On a donc représenté sur la figure 1 le schéma fonctionnel d'une carte à microprocesseur susceptible de mettre en œuvre le procédé selon l'invention.

La carte C comporte une unité principale de traitement 1, des mémoires de programmes 3 et 4 et une mémoire de travail (non représentée), associées à l'unité 1. La carte comporte également un processeur arithmétique 2 capable d'effectuer des calculs d'exponentiation modulaire. Il pourra s'agir par exemple de circuits tels que le circuit ST16CF54 commercialisé par la société STMicroelectronics ou 83C852/5 de la société Philips. La carte possède également un générateur de nombres entiers aléatoires 5.

Selon l'invention, l'opération de vérification de la co-primalité des nombres entiers a et b est réalisée par les étapes A et B indiquées sur le schéma de la figure 2, avec l'étape de retenue du couple a, b pour générer une clé électronique dans le cas où ces nombres sont premiers entre eux. En pratique cette étape consiste à stocker le couple a, b dans la mémoire sécuri-

sée 6 (non accessible de l'extérieur) du processeur arithmétique 2.

Avant de décrire l'exemple d'implémentation du procédé selon l'invention dans le cas du protocole RSA, on rappelle que la fonction λ est la fonction de Carmichael et que cette fonction est définie par la relation suivante :

$\lambda(b) = PPCM(\lambda(p^{\delta_1}), \quad , (\lambda(p^{\delta_k}))$,

dans laquelle PPCM désigne le plus petit commun multiple,

dans laquelle $b = \Pi p_i^{\delta_i}$ où chaque p_i est un nombre premier et chaque δ_i un entier positif non nul et $1<i<k$.

Dans l'exemple illustré du protocole de cryptographie RSA on procède aux étapes suivantes :

- stockage du nombre entier b choisi de longueur donnée fixée, (10)
- calcul de $\lambda(b)$ (20)
- stockage du nombre $\lambda(b)$ (30)

Ces étapes peuvent être préalables aux étapes qui suivent dans la mesure où b serait connu d'avance. Dans ce cas la valeur $\lambda(b)$ pré calculée sera stockée en mémoire sécurisée 6 du processeur arithmétique 5.

- tirage d'un nombre entier aléatoire a (40)
- calcul de $a^{\lambda(b)} \bmod b$ (50)
- comparaison de $a^{\lambda(b)} \bmod b$ à 1 (60)
- s'il y a égalité, stockage du couple (a, b) pour générer une clé du protocole de cryptographie, (70)
- s'il n'y a pas d'égalité (80)

réitération des étapes précédentes à partir du tirage d'un nouveau nombre entier a.

REVENDICATIONS

1. Procédé de génération de clés électroniques à partir de deux nombres entiers a, b, le procédé comprenant une étape de vérification de la co-primalité desdits nombres a, b, caractérisé en ce que cette étape de vérification comprend les opérations suivantes :

A) - calcul de l'exponentiation, modulaire $a^{\lambda(b)}$modb, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

C) - on retient le couple a, b lorsque l'égalité est vérifiée et on réitère avec un autre couple dans le cas contraire.

2. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que :

- on choisit un nombre entier b d'une longueur donnée et on le mémorise,
- on tire au hasard un nombre entier a,
- on calcule $a^{\lambda(b)}$modb
- on vérifie que $a^{\lambda(b)} = 1$ modb (ou $a^{\lambda(b)}$modb = 1),
- on mémorise le nombre a dans le cas où l'égalité est vérifiée,
- on réitère les étapes précédentes avec un autre nombre a dans le cas contraire.

3. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

4. Procédé de génération de clés cryptographiques RSA ou El Gamal ou Schnorr, caractérisé en ce qu'il met en œuvre le procédé selon l'une quelconque des revendications précédentes.

5. Dispositif électronique portable comprenant un processeur arithmétique et une mémoire de programme associée, apte à effectuer des exponentiations modulaires, caractérisé en ce qu'il comprend un programme de vérification de co-primalité de nombres entiers de longueur donnée qui effectue les opérations suivantes :

A) - calcul de l'exponentiation modulaire $a^{\lambda(b)}$modb, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

D) le processeur arithmétique stocke le couple a, b lorsque l'égalité est vérifiée et réitère avec un autre couple dans le cas contraire.

6. Dispositif électronique portable selon la revendication 5, caractérisé en ce que dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

7. Dispositif électronique portable selon la revendication 5 ou 7, caractérisé en ce qu'il est constitué par une carte à puce à microprocesseur.

Fig. 1

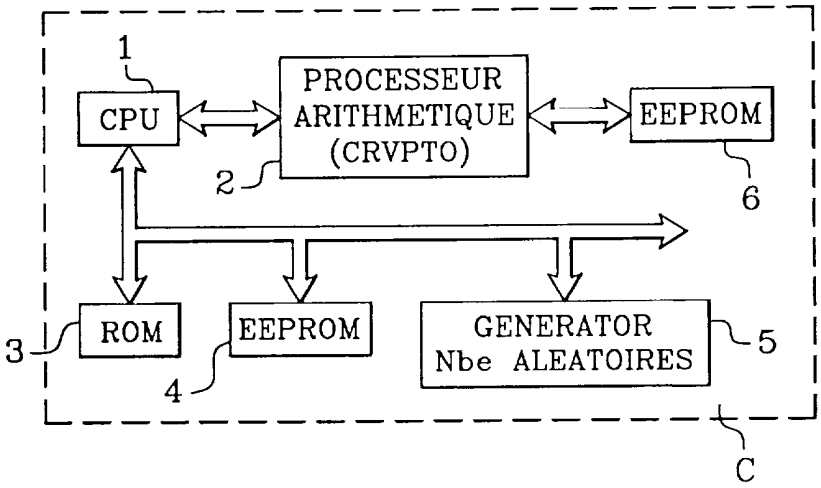
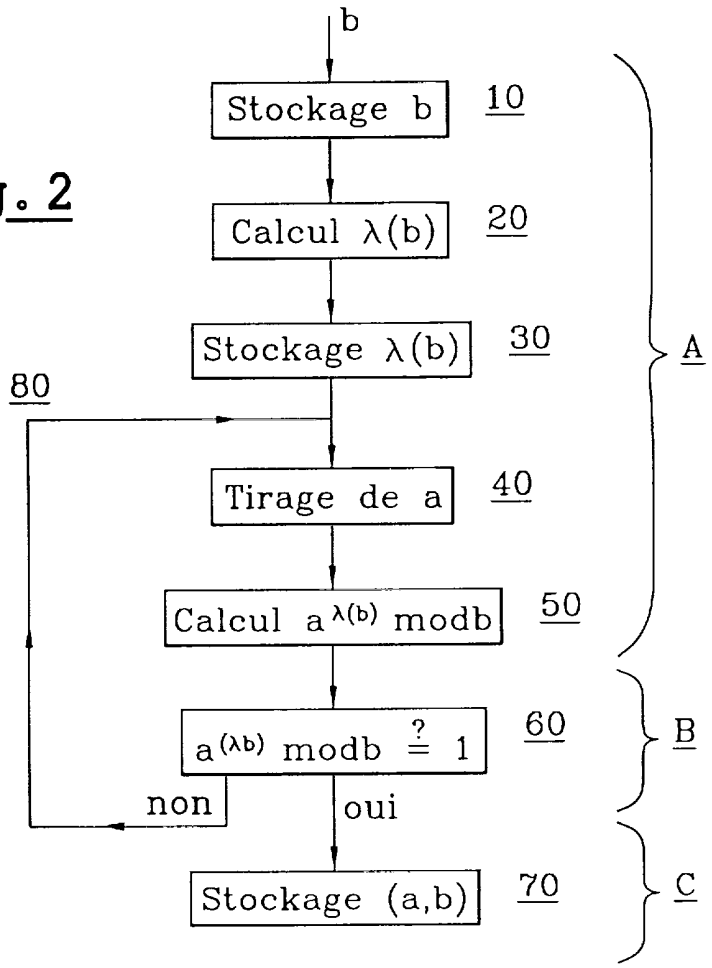

1
CPU
PROCESSEUR
ARITHMETIQUE
(CRVPTO)
2
EEPROM
6
3
ROM
EEPROM
4
GENERATOR
Nbe ALEATOIRES
5
C

Fig. 2


b
Stockage b
10
Calcul λ(b)
20
Stockage λ(b)
30
A
80
Tirage de a
40
Calcul a^λ(b) modb
50
a^(λb) modb ? = 1
60
B
non
oui
Stockage (a,b)
70
C

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2807246

N° d'enregistrement national

FA 584377
FR 0003919

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

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	MENEZES A J; VAN OORSCHOT P; VANSTONE S: "Handbook of Applied Cryptography" 1997 , CRC PRESS , BOCA RATON, FLORIDA 33431, USA XP002155110 ISBN: 0-8493-8523-7 * page 133 - page 134 * * page 138 * ---	1-7	H04L9/30
A	HARALD F; CHRISTIAN S: "Power permutations on prime residue classes" COMMUNICATIONS AND MULTIMEDIA SECURITY; PROCEEDINGS OF THE IFIP TC6, TC11 AND AUSTRIAN COMPUTER SOCIETY JOINT WORKING CONFERENCE ON COMMUNICATIONS AND MULTIMEDIA SECURITY, septembre 1995 (1995-09), pages 191-197, XP000972383 ISBN: 0-412-73260-2 * page 192, ligne 21 * -----	1,2,5	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04L

Date d'achèvement de la recherche	Examinateur
11 décembre 2000	Carnerero Álvaro, F

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

EPO FORM 1503 12.99 (P04C14)