(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
25 janvier 2001 (25.01.2001)

PCT

(10) Numéro de publication internationale
WO 01/06351 A1

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

(21) Numéro de la demande internationale:
PCT/FR00/02010

(22) Date de dépôt international: 12 juillet 2000 (12.07.2000)

(25) Langue de dépôt: français

(26) Langue de publication: français

(30) Données relatives à la priorité:
99/09317 15 juillet 1999 (15.07.1999) FR

(71) Déposant *(pour tous les États désignés sauf US)*: **GEMPLUS** [FR/FR]; Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)*: **CORON, Jean-Sébastien** [FR/FR]; 4, rue Léon de Lagrange, F-75015 Paris (FR). **HAN, Yong-Fei** [SG/SG]; Blk#07-239, Chao chu kang, Avenue 2, Singapore 680274 (SG). **ZHANG, Jiang** [SG/SG]; Blk#07-239, Chao chu kang, Avenue 2, Singapore 680274 (SG).

(74) Mandataire: **BRUYERE, Pierre**; Gemplus, Parc d'activités de Gémenos, Avenue du Pic de Bertagne, F-13881 Gémenos (FR).

(81) États désignés *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, 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, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

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

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.

(54) Title: METHOD FOR IMPROVING THE PERFORMANCE OF A MULTIPLICATION OPERATION ON A FINITE CHARACTERISTIC 2 BODY

(54) Titre: PROCEDE D'AMELIORATION DE PERFORMANCE DE L'OPERATION DE MULTIPLICATION SUR UN CORPS FINI DE CARACTERISTIQUE 2

(57) Abstract: Elliptic curve-based algorithms are public key algorithms having over RSA the advantage of less computing time and smaller sized keys. Their implementation in a smart card environment requires efficient algorithm computation. The inventive method consists in a method for rapid calculation of the operation for multiplying co-ordinates of a point pertaining to an elliptic curve.

(57) Abrégé: Les algorithmes cryptographiques à base de courbes elliptiques sont des algorithmes à clef publique présentant sur RSA l'avantage de temps de calcul plus faible et de taille de clefs plus petites. Leur implémentation dans le cadre d'environnement de type carte à puce nécessite des algorithmes de calcul efficaces. Le procédé de l'invention consiste en une méthode de calcul rapide de l'opération de multiplication des coordonnées d'un point appartenant à une courbe elliptique.

WO 01/06351 A1

PROCEDE D'AMELIORATION DE PERFORMANCE DE L'OPERATION DE MULTIPLICATION SUR UN CORPS FINI DE CARACTERISTIQUE 2

La présente invention concerne un procédé d'amélioration de performance de l'opération de multiplication dans un corps fini de caractéristique deux (corps fini de la forme GF(2^n), n étant un entier). Cette opération est fréquemment utilisée dans le cadre de la cryptographie à base de courbe elliptique.
Elle est particulièrement destinée à être mise en oeuvre dans des dispositifs électroniques du type carte à puce, PCMCIA, badges, cartes sans contact ou tout autre appareil portable

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

il est impossible de connaître ou de modifier les informations qui transitent par ledit canal. Un tel canal sécurisé peut être réalisé par un câble reliant deux terminaux, possédés par les deux dites personnes.

Le concept de cryptographie à clef publique fut inventé par Whitfield DIFFIE et Martin HELLMAN en 1976. La cryptographie à clef publique permet de résoudre le problème de la distribution des clefs à travers un canal non sécurisé. Le principe de la cryptographie à clef publique consiste à utiliser une paire de clefs, une clef publique de chiffrement et une clef privée de déchiffrement. Il doit être calculatoirement infaisable de trouver la clef privée de déchiffrement à partir de la clef publique de chiffrement. Une personne A désirant communiquer une information à une personne B utilise la clef publique de chiffrement de la personne B. Seule la personne B possède la clef privée associée à sa clef publique. Seule la personne B est donc capable de déchiffrer le message qui lui est adressé.

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

La première réalisation de schéma de chiffrement à clef publique fut mis au point en 1977 par

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

- Sac à dos de Merckle-Hellman :
  Ce système de chiffrement est basé sur la difficulté du problème de la somme de sous-ensembles.

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

- ElGamal :
  Ce système de chiffrement est basé sur la difficulté du logarithme discret dans un corps fini.

- Courbes elliptiques :
  Le système de chiffrement à courbe elliptique constitue une modification de systèmes cryptographiques existant pour les appliquer au domaine des courbes elliptiques.

L'utilisation de courbes elliptiques dans des systèmes cryptographiques fut proposé

indépendamment par Victor Miller et Neal Koblitz en 1985. Les applications réelles des courbes elliptiques ont été envisagées au début des années 1990. L'avantage de cryptosystèmes à base de courbe elliptique est qu'ils fournissent une sécurité équivalente aux autres cryptosystèmes mais avec des tailles de clef moindres. Ce gain en taille de clé implique une diminution des besoins en mémoire et une réduction des temps de calcul, ce qui rend l'utilisation des courbes elliptiques particulièrement adaptées pour des applications de type carte à puce.

Une courbe elliptique sur un corps fini GF(q^n) (q étant un nombre premier et n un entier) est l'ensemble des points (x,y) avec x l'abscisse et y l'ordonnée appartenant à GF(q^n) solution de l'équation :

$$y^2=x^3+a*x+b$$

si q est supérieur ou égal à 3

et

$$y^2+x*y=x^3+a*x^2+b$$

si q=2.

Il existe deux procédés pour représenter un point d'une courbe elliptique :

Premièrement, la représentation en coordonnées affine; dans ce procédé, un point P de la courbe elliptique est représenté par ses coordonnées (x,y).

Deuxièmement, la représentation en coordonnées projectives.

L'avantage de la représentation en coordonnées projectives est qu'elle permet d'éviter les divisions dans le corps fini, lesdites divisions étant les opérations les plus coûteuses en temps de calcul.

La représentation en coordonnés projectives le plus couramment utilisée est celle consistant à représenter un point P de la courbe elliptique par les coordonnées (X,Y,Z), telles que x=X/Z et y=Y/Z^3.

Les coordonnées projectives d'un point ne sont pas uniques parce que le triplet (X,Y,Z) et le triplet (λ^2*X, λ^3*Y, λ*Z) représentent le même point quelque soit l'élément λ appartenant au corps fini sur lequel est défini la courbe elliptique.

Les deux classes de courbes les plus utilisées en cryptographie sont les suivantes :

1) Courbes définies sur le corps fini GF(p) (ensemble des entiers modulo p, p étant un nombre premier) ayant pour équation $y^2=x^3+a*x+b$, a et b étant 2 éléments du corps fini GF(p).

2) Courbes définies sur le corps fini $GF(2^n)$ (ensemble des polynômes de degré inférieur ou égal à n-1 à coefficients 0 ou 1) ayant pour équation
$y^2+x*y=x^3+a*x^2+b$, a et b étant 2 éléments du corps fini $GF(2^n)$.

Pour chacune de ces deux classes de courbes, on définit les opérations d'addition de point et de doublement de point.

L'addition de point consiste en l'opération qui étant donné deux points P et Q calcule la somme R=P+Q, R étant un point de la courbe dont les coordonnées s'expriment à l'aide des coordonnées des points P et Q suivant des formules dont l'expression est donnée dans l'ouvrage " Elliptic curve public key cryptosystem " par Alfred J. Menezes.
Le doublement de point est l'opération qui, étant donné un point P, calcule le point R=2*P, R étant un point de la courbe dont les coordonnées s'expriment à l'aide des coordonnées du point P suivant des formules dont l'expression est donnée dans l'ouvrage " Elliptic curve public key cryptosystem " par Alfred J. Menezes.

Les opérations sur les coordonnées des points appartenant à la courbe elliptique sont des opérations portant sur des éléments appartenant à un corps fini de type GF(p) ou $GF(2^n)$. Les opérations définies sur le corps fini sont les 3

opérations suivantes : opération d'addition, opération de multiplication, opération d'inversion.

L'opération de multiplication sur un corps fini du type GF(2^n) est généralement constituée de deux étapes, la première étape consistant en la multiplication des deux polynômes représentant les deux éléments appartenant au corps fini, la deuxième étape consistant en la réduction modulaire du polynôme obtenu.

L'opération traditionnelle de multiplication de deux polynômes représentant deux éléments définis sur un corps fini GF(2^n) consiste en les opérations suivantes, l'algorithme prenant en entrée
deux éléments a et b appartenant au corps fini GF(2^n), a=a(n-1)*t^(n-1)+…+a(1)*t+a(0) et b=b(n-1)*t^(n-2)+…+b(1)*t+b(0), t étant le coefficient indéterminé du polynôme, les coefficients a(i) et b(i) pour i compris entre 0 et n-1 étant égaux à 0 ou à 1 :

1) Initialiser la variable c à 0.
2) Pour i allant de n-1 à 0 faire
   2)a) Remplacer c par t*c
   2)b) Si a(i) est différent de 0, ajouter le polynôme b au polynôme c.
3) Renvoyer en sortie le polynôme c.

L'inconvénient de l'algorithme précédent est qu'il nécessite une opération de rotation du

polynôme c lors de l'exécution de l'opération 2)a). Si le polynôme c est représenté sur des registres comprenant w bits, chaque opération de rotation du polynôme nécessite approximativement 2*n/w rotations de registre. Le nombre total de rotations de registre lors de l'exécution de l'algorithme précédant est donc approximativement 2*n*n/w.

Le procédé de l'invention consiste en un algorithme amélioré de multiplication de polynômes représentant des éléments appartenant à un corps fini de type $GF(2^n)$, ledit procédé permettant une réduction du nombre de rotations de registre au cours de l'exécution de l'algorithme et permettant ainsi d'obtenir un temps d'exécution plus court. Le procédé prend en entrée deux polynômes a et b représentant un élément du corps fini de type GF(2^n), notés a=a(n-1)*t^(n-1)+…+a(1)*t+a(0) et b=b(n-1)*t^(n-2)+…+b(1)*t+b(0), les coefficients a(i) et b(i) pour i compris entre 0 et n-1 étant égaux à 0 ou à 1. Le procédé utilise comme variable de calcul un polynôme c. On note C[j] le registre numéro j de la représentation du polynôme c. On note A[j] le registre numéro j de la représentation du polynôme a. On note w le nombre de bits dans un registre et s le nombre de registres nécessaires à la représentation d'un polynôme. Le procédé de multiplication de polynôme amélioré comprend les six étapes suivantes :

1) Initialisation du polynôme c à 0.
2) Pour j allant de w-1 à 0 exécuter les étapes suivantes
   2)a) Pour k allant de 1 à s exécuter l'opération 2)b)
   2)b) Si b(k*w-1)=1 alors exécuter l'opération suivante :
   Pour i allant de s-1+k-1 à k-1 remplacer le registre C[i] par le résultat de l'opération de ou exclusif entre le registre C[i] et le registre A[i-k+1]
3) Décaler tous les registres représentant le polynôme c d'un bit vers la gauche.
4) Décaler tous les registres représentant le polynôme b d'un bit vers la gauche
5) Retourner à l'étape 2)
6) Renvoyer en sortie le polynôme c.

Le nombre de rotation de polynôme nécessaires pour l'exécution de l'algorithme est donc approximativement égal à 2*n, ce qui représente une accélération par rapport à l'algorithme de multiplication classique.

Le procédé de l'invention consiste également en une amélioration du procédé de réduction modulaire utilisé dans le procédé de multiplication de deux éléments appartenant à un corps fini $GF(2^n)$.

Le procédé généralement utilisé pour réaliser l'opération de réduction modulaire est le suivant. Le procédé prend en entrée un polynôme

a noté a=a(2*n-1)*t^(2*n-1)+…+a(1)*t+a(0) de degré inférieur ou égal à 2*n-1 et renvoie en sortie un élément c du corps fini GF(2^n) noté c=c(n-1)*t^(n-2)+…+c(1)*t+c(0). On note C[j] le registre numéro j de la représentation du polynôme c. On note A[j] le registre numéro j de la représentation du polynôme a. Le polynôme utilisé lors de la réduction modulaire est de la forme t^n+t^k+1, k étant un paramètre entier. On note w la taille des registres en bit et s le nombre de registres. Le procédé est caractérisé par les dix étapes suivantes :

1) Calculer p=n-k modulo w
2) Calculer q=(n-k)/w
3) Initialiser la variable temp à 0
4) Initialiser la variable mask à (-1) << (n mod w), l'opération << (n mod w) dénotant la rotation de n mod w bits vers la gauche.
5) Pour j allant de 2*s-1 à s faire :
   5)a) Remplacer A[j-q] par A[j-q]+(A[j] >> p), l'opération >> p dénotant la rotation de p bits vers la droite.
   5)b) Remplacer A[(j-q)-1] par A[(j-q)-1]+(A[j] << (w-p))
6) Remplacer temp par A[s-1] xor mask
7) Remplacer A[(s-1)-q] par A[(s-1)-q] xor (temp >> p)
8) Remplacer A[(s-1)-q-1] par A[(s-1)-q-1] xor (temp << (w-p))
9) Remplacer C[i] par A[i] pour i allant de 0 à s-1
10) Renvoyer en sortie le polynôme c.

Le procédé de réduction modulaire amélioré de l'invention prend en entrée un polynôme a noté a=a(2*n-1)*t^(2*n-1)+...+a(1)*t+a(0) de degré inférieur ou égal à 2*n-1 et renvoie en sortie un élément c du corps fini GF(2^n) noté c=c(n-1)*t^(n-2)+...+c(1)*t+c(0) , les coefficients a(i) et c(i) pour i compris entre 0 et 2*n-1 étant égaux à 0 ou à 1. On note C[j] le registre numéro j de la représentation du polynôme c. On note A[j] le registre numéro j de la représentation du polynôme a. Le polynôme utilisé lors de la réduction modulaire est de la forme t^n+t^k+1, k étant un paramètre entier. On note w la taille des registres en bit et s le nombre de registres. Le procédé de réduction modulaire amélioré est caractérisé par les dix huit étapes suivantes :

1) Calculer p=n-k modulo w
2) Calculer q=(n-k)/w
3) Initialiser les variables temp1 et temp2 à 0
4) Décaler les registres A[2*s-1] à A[2*s-1-s/2] de p bits vers la droite.
5) Décaler la variable temp1 de un bit vers la droite.
6) Pour j allant de 2*s-1 à 2*s-1-s/2 remplacer A[j-q] par A[j-q] xor A[j]
7) Remplacer A[2*s-1-s/2-q-1] par A[2*s-1-s/2-q-1] xor temp1
8) Décaler les registres A[2*s-1] à A[2*s-1-s/2] de p bits vers la droite.

9) Décaler la variable temp1 de un bit vers la droite.

10) Pour j allant de s-1+s/2 à s remplacer A[j-q] par A[j-q] xor A[j]

11) Remplacer A[s-q-1] par A[s-q-1] xor temp1

12) Initialiser mask à (-1) << (n mod w), l'opération << (n mod w) dénotant la rotation de n mod w bits vers la gauche.

13) Remplacer temp1 par A[s-1] and mask.

14) Pour i allant de p à 1 faire

14)a) Décaler le polynôme temp1 de 1 bit vers la droite

14)b) Décaler le polynôme temp2 de 1 bit vers la droite

15) Remplacer A[(s-1)-q] par A[(s-1)-q] xor temp1

16) Remplacer A[(s-1)-q-1] par A[(s-1)-q-1] xor temp2

17) Remplacer C[i] par A[i] pour i allant de 0 à s-1

18) Renvoyer en sortie le polynôme c.

Les procédés de multiplication de polynômes et de réduction modulaire décrits précédemment permettent donc d'améliorer l'efficacité du procédé de multiplication de deux éléments dans un corps fini de caractéristique 2.

REVENDICATIONS

1- Procédé de multiplication de polynômes amélioré destiné à être implémenté dans un dispositif électronique portable, ledit procédé prenant en entrée deux polynômes a et b représentant un élément d'un corps fini de type GF(2^n), notés a=a(n-1)*t^(n-1)+...+a(1)*t+a(0) et b=b(n-1)*t^(n-2)+...+b(1)*t+b(0), les coefficients a(i) et b(i) pour i compris entre 0 et n-1 étant égaux à 0 ou à 1, ledit procédé utilisant comme variable de calcul un polynôme c, les registres de la représentation des polynômes c et a étant notés respectivement C[j] et A[j] pour le registre numéro j, le nombre de bits dans chaque registre étant noté w, le nombre de registres nécessaires à la représentation d'un polynôme étant noté s, caractérisé en ce qu'il comprend les six étapes suivantes :

1) Initialisation du polynôme c à 0.
2) Pour j allant de w-1 à 0 exécuter les étapes suivantes
   2)a) Pour k allant de 1 à s exécuter l'opération 2)b)
   2)b) Si b(k*w-1)=1 alors exécuter la sous étape suivante :
   Pour i allant de s-1+k-1 à k-1 remplacer le registre C[i] par le résultat de l'opération de ou exclusif entre le registre C[i] et le registre A[i-k+1]

3) Décaler les registres représentant le polynôme c d'un bit vers la gauche
4) Décaler les registres représentant le polynôme b d'un bit vers la gauche
5) Retourner à l'étape 2)
6) Renvoyer en sortie le polynôme c.

2- Procédé de réduction modulaire amélioré destiné à être implémenté dans un dispositif élecronique portable, ledit procédé prenant en entrée un polynôme a noté a=a(2*n-1)*t^(2*n-1)+…+a(1)*t+a(0) de degré inférieur ou égal à 2*n-1 et renvoyant en sortie un élément c du corps fini $GF(2^n)$ noté c=c(n-1)*t^(n-2)+…+c(1)*t+c(0), les coefficients a(i) et c(i) pour i compris entre 0 et 2*n-1 étant égaux à 0 ou à 1, les registres de la représentation des polynômes c et a étant notés respectivement C[j] et A[j] pour le registre numéro j, le nombre de bits dans chaque registre étant noté w, le nombre de registres nécessaires à la représentation d'un polynôme étant noté s, le polynôme utilisé lors de la réduction modulaire étant de la forme t^n+t^k+1, k étant un paramètre entier, le nombre de registres nécessaires à la représentation d'un polynôme étant noté s, caractérisé en ce qu'il comprend les dix huit étapes suivantes :

1) Calculer p=n-k modulo w
2) Calculer q=(n-k)/w

3) Initialiser les variables temp1 et temp2 à 0

4) Décaler les registres A[2*s-1] à A[2*s-1-s/2] de p bits vers la droite.

5) Décaler la variable temp1 de un bit vers la droite.

6) Pour j allant de 2*s-1 à 2*s-1-s/2 remplacer A[j-q] par A[j-q] xor A[j]

7) Remplacer A[2*s-1-s/2-q-1] par A[2*s-1-s/2-q-1] xor temp1

8) Décaler les registres A[2*s-1] à A[2*s-1-s/2] de p bits vers la droite.

9) Décaler la variable temp1 de un bit vers la droite.

10) Pour j allant de s-1+s/2 à s remplacer A[j-q] par A[j-q] xor A[j]

11) Remplacer A[s-q-1] par A[s-q-1] xor temp1

12) Initialiser mask à (-1) << (n mod w), l'opération << (n mod w) dénotant la rotation de n mod w bits vers la gauche.

13) Remplacer temp1 par A[s-1] and mask.

14) Pour i allant de p à 1 faire

14)a) Décaler le polynôme temp1 de 1 bit vers la droite

14)b) Décaler le polynôme temp2 de 1 bit vers la droite

15) Remplacer A[(s-1)-q] par A[(s-1)-q] xor temp1

16) Remplacer A[(s-1)-q-1] par A[(s-1)-q-1] xor temp2

17) Remplacer C[i] par A[i] pour i allant de 0 à s-1

18) Renvoyer en sortie le polynôme c.

3 - Procédé de multiplication de deux éléments d'un corps fini de caractéristique 2 (corps fini de la forme GF(2^n)) destiné à être implémenté dans un dispositif électronique portable, caractérisé en ce qu'il utilise l'une quelconque des revendications 1 et 2.

4- Dispositif électronique utilisant le procédé selon l'une quelconque des revendications précédentes caractérisé en ce qu'il est un dispositif portable.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR 00/02010

A. CLASSIFICATION OF SUBJECT MATTER

CIB 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)

CIB 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 practicable, search terms used)

EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MIYAJI A ET AL: "Efficient elliptic curve exponentiation" INFORMATION AND COMMUNICATIONS SECURITY. FIRST INTERNATIONAL CONFERENCE, ICIS '97. PROCEEDINGS, INFORMATION AND COMMUNICATIONS SECURITY. FIRST INTERNATIONAL CONFERENCE, ICICS '97, BEIJING, CHINA, 11-14 NOV. 1997, pages 282-290, XP000865761 1997, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-63696-X page 285 --- -/--	1

[X] Further documents are listed in the continuation of Box C. [ ] See patent family 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
6 November 2000	22 November 2000
Name and mailing address of the ISA/	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR 00/ 02010

C. (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE WIN E ET AL: "A fast software implementation for arithmetic operations in GF(2)" LECTURE NOTES IN COMPUTER SCIENCE, US, SPRINGER VERLAG, NEW YORK, NY, 1996, pages 65-76, XP002081362 ISSN: 0302-9743 Page 67, paragraph 4 - page 70, paragraph 1 Page 73, paragraph 2 - page 74, paragraph 2 ----------	1
A	KOC C K ET AL : "FAST SOFTWARE EXPONENTIATION IN GF (2K)" IEEE SYMPOSIUM ON COMPUTER ARITHMETIC, US, LOS ALAMITOS, CA : IEEE COMP. SOC. PRESS, 6 July 1997 (06.07.97), pages 225-231, XP000788129 ISBN: 0-8186-7846-1 Page 228, right column, line 20 - line 35 Page 227, right column, line 22 - line 30 ----------	1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FR 00/02010

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

The search was limited since the International Searching Authority is not sufficiently equipped to search prior art concerning computer programmes (PCT Rule 39.1 (vi).

2. [X] Claims Nos.: Claims nos; 2 and dependent claims
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

See supplemental sheet ADDITIONAL MATTER PCT/ISA/210

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

Continued from field I.2

Claim nos.: 2 and dependent claims

The role of the variables temp1 and temp2 is very unclear given that these variables always remain at zero (except temp1 from line 13). It is impossible to establish the subject matter of these claims without clarification as to how the modular reduction method that is described is carried out. According to PCT Art. 6, the lack of clarity in these claims is such that no meaningful search could be carried out.

The applicant is advised that patent claims relating to inventions for which no international search has been produced cannot normally be the subject of an international preliminary examination (PCT Rule 66.1(e)). As a general rule, the EPO in its capacity as the authority entrusted with the task of carrying out an international preliminary examination will not conduct a preliminary examination for subjects in respect of which no search has been provided. This also applies to cases where the patent claims were amended after receipt of the international search report (PCT Article 19) or to cases where the applicant presents new patent claims in the course of the PCT Chapter II procedure.

RAPPORT DE RECHERCHE INTERNATIONALE

De ıde Internationale No
PCT/FR 00/02010

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, 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	MIYAJI A ET AL: "Efficient elliptic curve exponentiation" INFORMATION AND COMMUNICATIONS SECURITY. FIRST INTERNATIONAL CONFERENCE, ICIS '97. PROCEEDINGS, INFORMATION AND COMMUNICATIONS SECURITY. FIRST INTERNATIONAL CONFERENCE, ICICS '97, BEIJING, CHINA, 11-14 NOV. 1997, pages 282-290, XP000865761 1997, Berlin, Germany, Springer-Verlag, Germany ISBN: 3-540-63696-X page 285 --- -/--	1

[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
6 novembre 2000	22. 11. 2000

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

3

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	DE WIN E ET AL: "A fast software implementation for arithmetic operations in GF(2)" LECTURE NOTES IN COMPUTER SCIENCE,US,SPRINGER VERLAG, NEW YORK, NY, 1996, pages 65-76, XP002081362 ISSN: 0302-9743 page 67, alinéa 4 -page 70, alinéa 1 page 73, alinéa 2 -page 74, alinéa 2 ---	1
A	KOÇ Ç K ET AL: "FAST SOFTWARE EXPONENTIATION IN GF(2K)" IEEE SYMPOSIUM ON COMPUTER ARITHMETIC,US,LOS ALAMITOS, CA: IEEE COMP. SOC. PRESS, 6 juillet 1997 (1997-07-06), pages 225-231, XP000788129 ISBN: 0-8186-7846-1 page 228, colonne de droite, ligne 20 - ligne 35 page 227, colonne de droite, ligne 22 - ligne 30 -----	1

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR 00/02010

Cadre I Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 1 de la première feuille)

Conformément à l'article 17.2)a), certaines revendications n'ont pas fait l'objet d'une recherche pour les motifs suivants:

1. [X] Les revendications n^os –
se rapportent à un objet à l'égard duquel l'administration n'est pas tenue de procéder à la recherche, à savoir:

L'administration chargée de la recherche internationale n'étant pas suffisamment outillée pour procéder à la recherche de l'état de la technique au sujet de programmes d'ordinateurs, la recherche a été limitée (règle 39.1 (vi) PCT).

2. [X] Les revendications n^os 2 et revendications dépendantes
se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier:

voir feuille supplémentaire SUITE DES RENSEIGNEMENTS PCT/ISA/210

3. [ ] Les revendications n^os
sont des revendications dépendantes et ne sont pas rédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

Cadre II Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 2 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir:

1. [ ] Comme toutes les taxes additionnelles ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. [ ] Comme toutes les recherches portant sur les revendications qui s'y prêtaient ont pu être effectuées sans effort particulier justifiant une taxe additionnelle, l'administration n'a sollicité le paiement d'aucune taxe de cette nature.

3. [ ] Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n^os

4. [ ] Aucune taxe additionnelle demandée n'a été payée dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n^os

Remarque quant à la réserve

[ ] Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant.

[ ] Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

SUITE DES RENSEIGNEMENTS INDIQUES SUR PCT/ISA/ 210

Suite du cadre I.2

Revendications nos.: 2 et revendications dépendantes

Le rôle des variables templ et temp2 est très douteux, étant donné que ces variables restent toujours à zéro (sauf templ à partir de ligne 13). En l'absence de clarification du déroulement du procédé de réduction modulaire décrit, il était impossible de comprendre l'objet de ces revendications. Suivant Art. 6 PCT, il y a absence de clarté dans ces revendications, au point que aucune recherche significative n'a été possible.

L'attention du déposant est attirée sur le fait que les revendications, ou des parties de revendications, ayant trait aux inventions pour lesquelles aucun rapport de recherche n'a été établi ne peuvent faire obligatoirement l'objet d'un rapport préliminaire d'examen (Règle 66.1(e) PCT). Le déposant est averti que la ligne de conduite adoptée par l'OEB agissant en qualité d'administration chargée de l'examen préliminaire international est, normalement, de ne pas procéder à un examen préliminaire sur un sujet n'ayant pas fait l'objet d'une recherche. Cette attitude restera inchangée, indépendamment du fait que les revendications aient ou n'aient pas été modifiées, soit après la réception du rapport de recherche, soit pendant une quelconque procédure sous le Chapitre II.