(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
3 janvier 2002 (03.01.2002)

PCT

(10) Numéro de publication internationale
WO 02/01343 A1

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

(21) Numéro de la demande internationale :
PCT/FR01/01943

(22) Date de dépôt international : 20 juin 2001 (20.06.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00/08279 26 juin 2000 (26.06.2000) FR

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

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

(74) Mandataire : **BRUYERE, Pierre**; Gemplus, Service brevets, Boîte postale 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, 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, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

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:** COUNTERMEASURE METHODS IN AN ELECTRONIC COMPONENT USING A KOBLITZ ELLIPTIC CURVE PUBLIC KEY CRYPTOGRAPHIC ALGORITHM

(54) **Titre :** PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE DE KOBLITZ

(57) **Abstract:** Cryptographic algorithms based on abnormal binary elliptic curves are public key algorithms having over RSA algorithms the advantage of less time calculation and smaller key size. It has been found that their application in a smart card type environment is vulnerable to DPA (Differential Power Analysis) attacks. The invention consists in the description of countermeasure methods to provide against such DPA attacks. Said countermeasure does not decrease performances and is easily used in a component such as a smart card.

(57) **Abrégé :** Les algorithmes cryptographiques à base de courbes elliptiques binaires anormales sont des algorithmes à clef publique présentant sur RSA l'avantage de temps de calcul plus faible et de taille de clefs plus petites. Il est apparu que leur application dans le cadre d'un environnement de type carte à puce était vulnérable à des attaques de type DPA (Differential Power Analysis). La présente invention consiste en la description de procédés de contre-mesures permettant de se prémunir contre ce type d'attaque DPA. Cette contre-mesure ne diminue pas les performances et est facilement utilisable dans un composant de type carte à puce.

WO 02/01343 A1

PROCEDES DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN ŒUVRE UN ALGORITHME DE CRYPTOGRAPHIE A CLE PUBLIQUE DE TYPE COURBE ELLIPTIQUE DE KOBLITZ

La présente invention concerne un procédé de contre-mesure dans un composant électronique mettant en œuvre un algorithme de chiffrement à clé publique de type courbe elliptique de Koblitz.

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 crypto systèmes à base de courbe elliptique est qu'ils fournissent une sécurité équivalente aux autres crypto systèmes 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(2^n) (n étant un entier) est l'ensemble des points (x,y) avec x l'abscisse et y l'ordonnée appartenant à GF(2^n) solution de l'équation :

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

On définit les opérations d'addition de point et de doublement de point.

L'addition de point est 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 d'addition de point et de doublement de point permettent de définir une opération de multiplication scalaire : étant donné un point P appartenant à une courbe elliptique et un entier d, le résultat de la multiplication scalaire de P par d est le point Q tel que Q=d*P=P+P+...+P d fois.

Il existe une famille de courbes elliptiques dites courbes binaires anormales ou courbes de Koblitz. Cette famille de courbes est définie par l'équation :

$y^2+x.y=x^3+a.x^2+1$

où a est un entier égal à 0 ou 1.

Cette famille de courbe présente la propriété suivante : si le point de coordonnées (x,y) appartient à la courbe, le point (x^2,y^2) appartient aussi à la courbe. On définit en conséquence l'opérateur Frobenius noté τ qui à tout point de coordonnées (x,y) associe le point de coordonnées (x^2,y^2). Selon une méthode décrite dans l'article " An improved Algorithm for Arithmetic on a Family of Elliptic Curves " de J.A. Solinas publié à la conférence " Crypto'97 ", il est possible de représenter tout entier d sous la forme d'une somme de puissances de τ :

$$d=\Sigma\ d_i\ \tau^i$$

où l'entier d_i vaut -1, 0, ou 1.

Il existe deux représentations possibles d'un élément de l'ensemble $GF(2^n)$. La première est appelée représentation polynomiale et consiste à représenter un élément x sous la forme d'un polynôme en t :

$$x=x_{n-1}t^{n-1}+\ldots+x_0$$

La deuxième représentation est la représentation en base normale, qui consiste à représenter un élément x sous la forme :

$$x=x_{n-1}\ .\theta^{(2^{n-1})}+\ldots+\ x_0$$

L'avantage de la représentation en base normale est que la mise au carré d'un élément est très rapide. L'avantage de la représentation en base polynomiale est que les opérations de multiplication et d'inversion sont plus rapides. Il est possible de passer d'une représentation en base polynomiale à une représentation en base normale. Des méthodes de conversion efficaces sont décrites dans l'article " Storage efficient finite field basis conversion " par B.S. Kaliski Jr. And Y.L.Yin publié à la conférence " SAC'98 ".

La sécurité des algorithmes de cryptographie sur courbes elliptiques est basée sur la difficulté du problème du

logarithme discret sur courbes elliptiques, ledit problème consistant à partir de deux points Q et P appartenant à une courbe elliptique E, de trouver, s'il existe, un entier x tel que Q=x*P.

Il existe de nombreux algorithmes cryptographiques basés sur le problème du logarithme discret. Ces algorithmes sont facilement transposables aux courbes elliptiques. Ainsi, il est possible de mettre en oeuvre des algorithmes assurant l'authentification, la confidentialité, le contrôle d'intégrité et l'échange de clé.

Un point commun à la plupart des algorithmes cryptographiques basés sur les courbes elliptiques est qu'ils comprennent comme paramètres une courbe elliptique définie sur un corps fini et un point P appartenant à cette courbe elliptique. La clé privée est un entier d choisi aléatoirement. La clef publique est un point de la courbe Q tel que Q=d*P. Ces algorithmes cryptographiques font généralement intervenir une multiplication scalaire dans le calcul d'un point R=d*T où d est la clef secrète.

Dans le paragraphe ci dessous, on décrit un algorithme de chiffrement à base de courbe elliptique. Ce schéma est analogue au schéma de chiffrement d'El Gamal. Un message m est chiffré de la manière suivante :

le chiffreur choisit un entier k aléatoirement et calcule les points k*P=(x1,y1) et k*Q=(x2,y2) de la courbe, et l'entier c= x2 + m. Le chiffré de m est le triplet (x1,y1,c).

Le déchiffreur qui possède d déchiffre m en calculant :

(x'2,y'2)=d(x1,y1) et m=c-x'2

Pour réaliser les multiplications scalaires nécessaires dans les procédés de calcul décrits précédemment, plusieurs algorithmes existent :

- Algorithme " double and add ";
- Algorithme " addition-soustraction "

- Algorithme avec chaînes d'addition ;
- Algorithme avec fenêtre ;
- Algorithme avec représentation signée.

Cette liste n'est pas exhaustive. L'algorithme le plus simple et le plus utilisé est l'algorithme " double and add ". L'algorithme " double and add " prend en entrée un point P appartenant à une courbe elliptique donnée et un entier d. L'entier d est noté d=(d(t),d(t-1),…,d(0)), où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. L'algorithme retourne en sortie le point Q=d.P.

L'algorithme " double and add " comporte les 3 étapes suivantes :

1) Initialiser le point Q avec la valeur P
2) Pour i allant de t-1 à 0 exécuter :
   2a) Remplacer Q par 2Q
   2b) Si d(i)=1 remplacer Q par Q+P
3) Retourner Q.

Dans le cas de l'utilisation d'une courbe elliptique binaire anormale (dite de Koblitz), il est possible de remplacer l'algorithme précédent par l'algorithme suivant plus efficace comportant les 3 étapes suivantes. L'entier d est représenté selon :

$d=\Sigma\ d_i\ \tau\hat{}i$ où l'entier d_i vaut -1, 0, ou 1 et $0\leq i<t$ où t est un paramètre entier. L'algorithme suivant est appelé algorithme " τ and substract ".

1) Initialiser le point Q avec la valeur $d_{t-1}P$
2) Pour i allant de t-2 à 0 exécuter :
   2a) Remplacer Q par τ.Q.
   2b) Si d_i=1 remplacer Q par Q+P.
   2c) Si d_i=-1 remplacer Q par Q-P.
3) Retourner Q.

L'avantage de l'algorithme décrit précédemment sur l'algorithme " Double and Add " décrit précédemment est que l'opération de doublement de Q de l'étape 2a) est remplacée par l'opération du Frobenius plus rapide.

Il est apparu que l'implémentation sur carte à puce d'un algorithme de chiffrement à clé publique du type courbe elliptique était vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé privée de déchiffrement. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation de courant du microprocesseur exécutant des instructions varie selon la donnée manipulée.

En particulier, lorsqu'une instruction manipule une donnée dont un bit particulier est constant, la valeur des autres bits pouvant varier, l'analyse de la consommation de courant liée à l'instruction montre que la consommation moyenne de l'instruction n'est pas la même suivant que le bit particulier prend la valeur 0 ou 1. L'attaque de type DPA permet donc d'obtenir des informations supplémentaires sur les données intermédiaires manipulées par le microprocesseur de la carte lors de l'exécution d'un algorithme cryptographique. Ces informations supplémentaires peuvent dans certain cas permettre de révéler les paramètres privés de l'algorithme de déchiffrement, rendant le système cryptographique non sûr.

Dans la suite de ce document on décrit un procédé d'attaque DPA sur un algorithme de type courbe elliptique réalisant une opération du type multiplication scalaire d'un point P par un entier d, l'entier d étant la clé secrète. Cette attaque permet de révéler directement la clé secrète d. Elle compromet donc gravement la sécurité de l'implémentation de courbes elliptiques sur une carte à puce.

La première étape de l'attaque est l'enregistrement de la consommation de courant correspondant à l'exécution de l'algorithme " double and add " décrit précédemment pour N points distincts P(1),…,P(N). Dans un algorithme à base de courbes elliptiques, le microprocesseur de la carte à puce va effectuer N multiplications scalaires d.P(1),…,d.P(N).

Pour la clarté de la description de l'attaque, on commence par décrire une méthode permettant d'obtenir la valeur du bit d(t-1) de la clé secrète d, où (d(t),d(t-1),…,d(0)) est la représentation binaire de d, avec d(t) le bit de poids fort et d(0) le bit de poids faible. On donne ensuite la description d'un algorithme qui permet de retrouver la valeur de d.

On groupe les points P(1) à P(N) suivant la valeur du dernier bit de l'abscisse de 4.P, où P désigne un des points P(1) à P(N). Le premier groupe est constitué des points P tels que le dernier bit de l'abscisse de 4.P est égal à 1. Le second groupe est constitué des points P tels que le dernier bit de l'abscisse de 4.P est égal à 0. On calcule la moyenne des consommations de courant correspondant à chacun des deux groupes, et on calcule la courbe de différence entre ces deux moyennes.

Si le bit d(t-1) de d est égal à 0, alors l'algorithme de multiplication scalaire précédemment décrit calcule et met en mémoire la valeur de 4.P. Cela signifie que lors de l'exécution de l'algorithme dans une carte à puce, le microprocesseur de la carte va effectivement calculer 4.P. Dans ce cas, dans le premier groupe de message le dernier bit de la donnée manipulée par le microprocesseur est toujours à 1, et dans le deuxième groupe de message le dernier bit de la donnée manipulée est toujours à 0. La moyenne des consommations de courant correspondant à chaque groupe est donc différente. Il apparaît donc dans la courbe de différence entre les 2 moyennes un pic de différentiel de consommation de courant.

Si au contraire le bit d(t-1) de d est égal à 1, l'algorithme d'exponentiation décrit précédemment ne calcule pas le point 4.P. Lors de l'exécution de l'algorithme par la carte à puce, le microprocesseur ne manipule donc jamais la donnée 4.P. Il n'apparaît donc pas de pic de différentiel de consommation.

Cette méthode permet donc de déterminer la valeur du bit d(t-1) de d.

L'algorithme décrit dans le paragraphe suivant est une généralisation de l'algorithme précédent. Il permet de déterminer la valeur de la clé secrète d.

On définit l'entrée par N points notés P(1) à P(N) correspondant à N calculs réalisés par la carte à puce et la sortie par un entier h.

Ledit algorithme s'effectue de la manière suivante en trois étapes :

1) Exécuter h=1 ;

2) Pour i allant de t-1 à 1, exécuter :

   2)1) Classer les points P(1) à P(N) suivant la valeur du dernier bit de l'abscisse de (4*h).P ;

   2)2) Calculer la moyenne de consommation de courant pour chacun des deux groupes ;

   2)3) Calculer la différence entre les 2 moyennes ;

   2)4) Si la différence fait apparaître un pic de différentiel de consommation, faire h=h*2 ; sinon faire h=h*2+1 ;

3) Retourner h.

L'algorithme précédent fournit un entier h tel que d=2*h ou d=2*h+1. Pour obtenir la valeur de d, il suffit ensuite de tester les deux hypothèses possibles. L'attaque de type DPA décrite permet donc de retrouver la clé privée d. Une attaque similaire est possible dans le cas de l'utilisation de courbe elliptique dite " courbe de Koblitz ".

L'invention consiste en la définition de 3 procédés de contre-mesures permettant de se prémunir contre les attaques par mesure de courant.

Le procédé de la première contre-mesure consiste à rendre aléatoire l'exécution de l'algorithme " τ and substract " décrit précédemment. Ce procédé permet d'exécuter une opération de multiplication scalaire. Ainsi l'algorithme s'exécute suivant des étapes de calculs différentes pour chaque nouvelle exécution et l'attaque décrite précédemment n'est plus possible. L'algorithme " τ and substract " modifié consiste en les 4 étapes suivantes. L'entier d est représenté selon :

$d=\Sigma\, d_i\, \tau^i$ où l'entier d_i vaut -1, 0, ou 1 et $0 \leq i < t$ où t est un paramètre entier. Soit u le nombre d'entiers i tels que d_i soit différent de 0.

1) Tirer aléatoirement un entier i compris entre 0 et t-1, tel que d_i soit différent de 0.

2) Initialiser le point Q avec la valeur $d_i\, \tau^i\, P$

1) Répéter u-1 fois :

3a) Tirer aléatoirement un entier i compris entre 0 et t-1, tel que d_i soit différent de 0,

et qui n'ait pas été tiré auparavant.

3b) Remplacer Q par $Q+d_i\, \tau^i\, P$

2) Retourner Q.

Le premier procédé de la contre-mesure comprend deux variantes. Dans la première variante, le point P est représenté en base polynomiale. Dans la deuxième variante, le point P est représenté initialement en base normale. Le calcul de $d_i\, \tau^i\, P$ s'effectue également en base normale, ce qui permet un calcul plus rapide qu'en base polynomiale. Le point $d_i\, \tau^i\, P$ est ensuite converti en base polynomiale.

Le procédé de la deuxième contre-mesure consiste à protéger l'opération de mise au carré d'un élément contre les attaques

par mesure de courant. Cette opération est utilisée en particulier dans l'application de l'opérateur de Frobenius tel que décrit précédemment. L'opération de mise au carré d'un élément dans un corps de caractéristique 2 est une opération linéaire : $(x+y)^2=x^2+y^2$. Le procédé de la deuxième contre-mesure consiste à remplacer l'opération de mise au carré d'un élément x par le procédé suivant en 3 étapes :

1) Tirer aléatoirement un élément r de $GF(2^n)$.

2) Calculer $y=x+r$

3) Calculer y^2 et r^2

4) Retourner y^2+r^2

Ainsi, l'élément r étant aléatoire, l'élément y l'est aussi, et l'opération de mise au carré de y et de r de l'étape 3 intervient sur des éléments aléatoires, ce qui la protège contre des attaques par mesure de courant.

Le procédé de la deuxième contre-mesure comprend deux variantes. Dans la première variante, les éléments x,y et r sont représentés en base polynomiale. Dans la deuxième variante, les éléments x,y et r sont représentés en base normale.

Le procédé de la troisième contremesure consiste à effectuer un masquage de l'algorithme " τ and substract " décrit précédemment. L'algorithme " τ and substract " permet de calculer le point d.P étant donné le point P et l'entier d. On suppose par la suite que l'entier d est un entier fixe connu à l'avance. Le procédé de la troisième contre-mesure consiste à pré stocker en mémoire des couples de points de la forme : (S_i, R_i) avec $S_i = d.R_i$

On note u le nombre de couples stockés.

Le procédé de la troisième contre-mesure consiste à remplacer l'algorithme " τ and substract " décrit précédemment par le procédé suivant en 6 étapes :

1) Tirer aléatoirement un entier i compris entre 1 et u.

2) Tirer aléatoirement un entier j compris entre 0 et n-1.

3) Calculer $P'=P+\tau^j R_i$

4) Calculer $Q'=d.P'$ en utilisant l'algorithme " τ and substract " décrit précédemment.

5) Calculer $Q=Q'-\tau^j S_i$

6) Retourner Q.

Le procédé de la troisième contre-mesure comprend une première variante dans laquelle les points R_i et S_i sont représentés en base polynomiale. Dans une deuxième variante, les points R_i et S_i sont représentés en base normale. Le calcul de $\tau^j R_i$ à l'étape 3) et le calcul de $\tau^j S_i$ s'effectuent en base normale. Les points $\tau^j R_i$ et $\tau^j S_i$ sont ensuite convertis en base polynomiale.

Les trois procédés de contre-mesures précédemment décrits permettent de protéger l'exécution d'un algorithme de multiplication scalaire sur courbe elliptique binaire anormale (dite de Koblitz) contre les attaques par mesure de courant. Il est possible d'utiliser simultanément deux ou trois de ces contre-mesures. Ces trois procédés peuvent être utilisés lors de l'exécution de tout protocole cryptographique basé sur les courbes elliptiques, en particulier un protocole d'échange de clef, un protocole de signature électronique ou un protocole de chiffrement. Ces trois procédés sont particulièrement destinés à être utilisés dans un environnement électronique de type carte à puce.

REVENDICATIONS

1) Procédé de contre-mesure dans un composant électronique exécutant une opération de multiplication scalaire d'un point P appartenant à une courbe elliptique binaire anormale, par un entier d représenté sous la forme

$d=\Sigma\ d_i\ \tau\hat{}i$ l'entier d_i valant -1, 0, ou 1, l'entier i étant tel que $0\leq i<t$, l'entier t étant un paramètre, l'entier u étant par définition le nombre d'entiers i tels que d_i soit différent de 0, le caractère τ désignant l'opérateur de Frobenius s'appliquant ladite courbe elliptique, ledit procédé étant caractérisé en ce qu'il comprend les 4 étapes suivantes :

1) Tirer aléatoirement un entier i compris entre 0 et t-1, tel que d_i soit différent de 0.

2) Initialiser le point Q avec la valeur $d_i\ \tau^i\ P$

3) Répéter u-1 fois :

3a) Tirer aléatoirement un entier i compris entre 0 et t-1, tel que d_i soit différent de 0,

et qui n'ait pas été tiré auparavant

3b) Remplacer Q par $Q+d_i\ \tau^i\ P$

4) Retourner Q.

2) Procédé de contre-mesure dans un composant électronique exécutant une opération de multiplication scalaire d'un point P appartenant à une courbe elliptique binaire anormale, par un entier d selon la revendication 1, caractérisé en ce que le point P est représenté en base polynomiale.

3) Procédé de contre-mesure dans un composant électronique exécutant une opération de multiplication scalaire d'un point P appartenant à une courbe elliptique binaire anormale, par un entier d selon la revendication 1, caractérisé en ce que le point P est représenté en base normale, le calcul de $d_i\ \tau^i\ P$ s'effectuant également en base normale, le point $d_i\ \tau^i\ P$ étant ensuite converti en base polynomiale.

4) Procédé de contre-mesure dans un composant électronique exécutant une opération de mise au carré d'un élément dans un corps de caractéristique 2 caractérisé en ce qu'il consiste à remplacer l'opération classique de mise au carré d'un élément x par le procédé comprenant les 4 étapes suivantes :

1) Tirer aléatoirement un élément r de GF(2^n).

2) Calculer y=x+r

1) Calculer y^2 et r^2

2) Retourner y^2+r^2

5) Procédé de contre-mesure selon la revendication 4, caractérisé en ce que les éléments x,y et r sont représentés en base polynomiale.

6) Procédé de contre-mesure selon la revendication 4, caractérisé en ce que les éléments x,y et r sont représentés en base normale.

7) Procédé de contre-mesure dans un composant électronique exécutant une opération de multiplication scalaire modifiée d'un point P appartenant à une courbe elliptique binaire anormale, par un entier d, ledit procédé utilisant un ensemble de u couples de points de la forme
(S_i, R_i) avec $S_i = d.R_i$ stockés en mémoire, caractérisé en ce qu'il comprend les 6 étapes suivantes :

1) Tirer aléatoirement un entier i compris entre 1 et u.

1) Tirer aléatoirement un entier j compris entre 0 et n-1.

2) Calculer $P'=P+\tau^j R_i$

3) Calculer $Q'=d.P'$ en utilisant un algorithme de multiplication scalaire. Calculer $Q=Q'-\tau^j S_i$

4) Retourner Q.

8) Procédé de contre-mesure selon la revendication 7, caractérisé en ce que les points R_i et S_i sont représentés en base polynomiale.

9) Procédé de contre-mesure selon la revendication 7, caractérisé en ce que les points R_i et S_i sont représentés en base normale, le calcul de $\tau^j R_i$ et de $\tau^j S_i$ s'effectuant en coordonnées normales, les point $\tau^j R_i$ et $\tau^j S$ étant ensuite convertis en base polynomiale

10) Protocole cryptographique basé sur l'utilisation d'une courbe elliptique binaire anormale utilisant le procédé suivant l'une quelconque des revendications précédentes.

11) Composant électronique utilisant le procédé selon l'une quelconque des revendications précédentes caractérisé en ce qu'il peut être une carte à puce.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01943

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, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards" PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOLUME 1717), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. FIRST INTERNATIONAL WORKSHOP, CHES'99, WORCESTER, MA, USA, 12-13 AUG. 1999, pages 144-157, XP000952221 1999, Berlin, Germany, Springer-Verlag ISBN: 3-540-66646-X page 156, paragraph 1 --- -/--	1-3

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 September 2001	27/09/2001

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

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

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01943

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	CORON J -S: "Resistance against differential power analysis for elliptic curve cryptosystems" PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOLUME 1717), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. FIRST INTERNATIONAL WORKSHOP, CHES'99, WORCESTER, MA, USA, 12-13 AUG. 1999, pages 292-302, XP000952243 1999, Berlin, Germany, Springer-Verlag, ISBN: 3-540-66646-X page 300, column 5 ---	4-11
X	GOUBIN L ET AL: "DES and differential power analysis. The "Duplication" method" PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOLUME 1717), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. FIRST INTERNATIONAL WORKSHOP, CHES'99, WORCESTER, MA, USA, 12-13 AUG. 1999, pages 158-172, XP000952192 1999, Berlin, Germany, Springer-Verlag ISBN: 3-540-66646-X	4-6
A	page 171, column 5 -page 172, column 3 ---	7-11
A	SOLINAS J A: "An improved algorithm for arithmetic on a family of elliptic curves" PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO'97. 17TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, USA, 17-21 AUG. 1997, 1997, pages 357-371, XP002136758 1997, Berlin, Germany, Springer-Verlag ISBN: 3-540-63384-7 cited in the application page 362, paragraph 3 -page 367, paragraph 1 -----	1-11

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/01943

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, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	MESSERGES T S ET AL: "Power analysis attacks of modular exponentiation in smartcards" PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOLUME 1717), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. FIRST INTERNATIONAL WORKSHOP, CHES'99, WORCESTER, MA, USA, 12-13 AUG. 1999, pages 144-157, XP000952221 1999, Berlin, Germany, Springer-Verlag ISBN: 3-540-66646-X page 156, alinéa 1 --- -/--	1-3

[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
20 septembre 2001	27/09/2001

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 01/01943

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
X	CORON J -S: "Resistance against differential power analysis for elliptic curve cryptosystems" PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOLUME 1717), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. FIRST INTERNATIONAL WORKSHOP, CHES'99, WORCESTER, MA, USA, 12-13 AUG. 1999, pages 292-302, XP000952243 1999, Berlin, Germany, Springer-Verlag, ISBN: 3-540-66646-X page 300, colonne 5 ---	4-11
X	GOUBIN L ET AL: "DES and differential power analysis. The "Duplication" method" PROCEEDINGS (LECTURE NOTES IN COMPUTER SCIENCE VOLUME 1717), CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. FIRST INTERNATIONAL WORKSHOP, CHES'99, WORCESTER, MA, USA, 12-13 AUG. 1999, pages 158-172, XP000952192 1999, Berlin, Germany, Springer-Verlag ISBN: 3-540-66646-X	4-6
A	page 171, colonne 5 -page 172, colonne 3 ---	7-11
A	SOLINAS J A: "An improved algorithm for arithmetic on a family of elliptic curves" PROCEEDINGS, ADVANCES IN CRYPTOLOGY - CRYPTO'97. 17TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, CA, USA, 17-21 AUG. 1997, 1997, pages 357-371, XP002136758 1997, Berlin, Germany, Springer-Verlag ISBN: 3-540-63384-7 cité dans la demande page 362, alinéa 3 -page 367, alinéa 1 -----	1-11