

(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
2 février 2006 (02.02.2006)

PCT

(10) Numéro de publication internationale
WO 2006/010692 A2

(51) Classification internationale des brevets :
G06F 7/72 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2005/053088

(22) Date de dépôt international : 29 juin 2005 (29.06.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0451468 8 juillet 2004 (08.07.2004) FR

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

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) : **CORON, Jean-Sébastien** [FR/FR]; 17 avenue d'Argenteuil, F-92600 ASNIERES SUR SEINE (FR).

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT,

AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

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 METHOD IN AN ELECTRICAL COMPONENT IMPLEMENTING A PUBLIC KEY ALGORITHM USING THE ELLIPTICAL CURVES FOR PROTECTION COUPLING CALCULATION ON SAID CURVES

(54) Titre : PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE METTANT EN OEUVRE UN ALGORITHME A CLE PUBLIQUE UTILISANT LES COURBES ELLIPTIQUES PERMETTANT LA PROTECTION DU CALCUL DE COUPLAGE SUR LES DITES COURBES

(57) Abstract: The invention concerns a countermeasure method in a secure electronic component or module implementing a public key algorithm using the elliptical curves for protecting the coupling calculation between two points belonging to an elliptical curve. During the method, the secure module generates one or more random numbers randomize the calculation, thereby providing protection against said attacks through current measurement.

(57) Abrégé : L'invention concerne un procédé de contre-mesure dans un composant électronique ou module sécurisé mettant en oeuvre un algorithme à clé publique utilisant les courbes elliptiques permettant la protection du calcul de couplage entre deux points appartenant à une courbe elliptique. Au cours du procédé, le module sécurisé génère un ou plusieurs aléas permettant de rendre le calcul aléatoire, ce qui assure une protection contre lesdites attaques par mesure de courant.

WO 2006/010692 A2

PROCEDE DE CONTRE-MESURE DANS UN COMPOSANT ELECTRONIQUE
METTANT EN ŒUVRE UN ALGORITHME A CLE PUBLIQUE UTILISANT
LES COURBES ELLIPTIQUES PERMETTANT LA PROTECTION DU
CALCUL DE COUPLAGE SUR LES DITES COURBES

L'invention concerne un procédé de contre-mesure dans un composant électronique mettant en oeuvre un algorithme à clé publique utilisant les courbes elliptiques permettant la protection d'un calcul
5 cryptographique. Le calcul cryptographique protégé est le calcul du couplage de deux points définis sur une courbe elliptique. L'invention est notamment intéressante pour la mise en oeuvre de protocoles cryptographiques dans une carte à puce ou plus généralement dans tout module de
10 calcul sécurisé (par exemple un module TPM pour "Trusted Platform Module » installé dans un PC non sécurisé) ou composant électronique.

Le calcul du couplage de deux points définis sur une courbe elliptique est assimilable à un procédé permettant
15 la mise en oeuvre de protocoles possédant des propriétés intéressantes sur le plan cryptographique. A titre d'exemple, on peut citer un protocole de chiffrement basé sur l'identité (Boneh et Franklin, « Identity-based encryption from the Weil pairing », Proceedings of Crypto
20 2001), un protocole d'échange de clef entre trois parties (A. Joux, "A one-round protocol for tripartite Diffie-Hellman," *Algorithm Number Theory Symposium -- ANTS-IV*, Lecture Notes on Computer Science 1838, Springer-Verlag (2000), pp. 385-394), un schéma de signature courte
25 (Boneh et Boyen, « Short signatures without random oracles », Proceedings of Eurocrypt 2004).

Une courbe elliptique est un ensemble de points ayant des caractéristiques communes. Etant donné deux points A et B appartenant à une courbe elliptique, il est possible d'additionner ces deux points pour en obtenir un troisième C tel que $C=A+B$. De plus, étant donné un point P et un entier k, il est possible de calculer $k.P=P+P+\dots+P$ (l'opération étant répétée k fois). Cette opération s'appelle multiplication scalaire par un entier k. Etant donné deux points A et B appartenant à une courbe elliptique, il est possible de calculer le couplage entre les points A et B, noté $\langle A, B \rangle$. Pour plus de détails sur les courbes elliptiques, on pourra se reporter notamment à la publication du brevet français FR 2 828 779. La mise en oeuvre classique d'une opération de couplage de type $C = \langle A, B \rangle$ est détaillée notamment dans le document "Identity based encryption from the 'Weil pairing" D. Boneh et M. Franklin, Proceedings of Crypto 2001, disponible à l'adresse internet : <http://crypto.stanford.edu/~dabo/abstracts/ibe.html>). Les points A, B que l'on cherche à coupler sont par exemple une clé, publique ou privée, et un message, à chiffrer ou à déchiffrer, dans le cadre d'un protocole de cryptographie à clés asymétriques.

Il est apparu que l'implémentation sur carte à puce d'un algorithme cryptographique était généralement vulnérable à des attaques consistant en une analyse différentielle de consommation de courant permettant de retrouver la clé secrète. Ces attaques sont appelées attaques DPA, acronyme pour Differential Power Analysis. Le principe de ces attaques DPA repose sur le fait que la consommation en courant du microprocesseur exécutant des

instructions varie selon la donnée manipulée. Ainsi, en observant cette consommation de courant, ou plus généralement toute émission électromagnétique générée par la carte, il est possible pour un attaquant de retrouver les données secrètes stockées à l'intérieur de la carte. En particulier, on peut montrer qu'une implémentation sans protection du calcul du couplage entre deux points définis sur une courbe elliptique est vulnérable à une attaque par mesure de courant. A titre d'exemple, dans le cas d'une implémentation sur une carte à puce d'un protocole de chiffrement basé sur l'identité, une attaque par mesure de courant permettrait à un attaquant de déchiffrer tous les messages reçus par le destinataire.

L'invention a pour but de protéger une implémentation d'un procédé de couplage de points sur courbe elliptique contre les attaques par mesure de courant, pour permettre l'utilisation sécurisée de protocoles cryptographiques basés sur le couplage de points dans un module sécurisé tel qu'un composant électronique du type carte à puce.

Ce but est atteint à l'aide d'un procédé de randomisation du calcul du couplage de points. Ce procédé de randomisation consiste à effectuer des calculs intermédiaires sur des données aléatoires, qui ne peuvent donner aucune information à un attaquant, même par mesure de courant. Ensuite, ces données, issues desdits calculs intermédiaires, sont recomposées entre elles pour fournir le résultat final du procédé de calcul.

Le procédé de l'invention utilise la propriété de bilinéarité de la fonction de couplage sur courbe elliptique. Cette propriété de bilinéarité peut s'écrire de la manière suivante :

$$5 \quad \langle A, B+C \rangle = \langle A, B \rangle + \langle A, C \rangle$$

et

$$\langle A+B, C \rangle = \langle A, C \rangle + \langle B, C \rangle$$

Pour plus de simplicité, dans la suite du brevet, les opérations effectuées dans cet ensemble seront notées additivement comme dans la notation précédente. Dans la
10 suite du brevet, on notera par G un point générateur d'un ensemble de points appartenant à une courbe elliptique, ledit ensemble étant appelé groupe et on notera par n le nombre de points dudit groupe.

15

Le procédé de l'invention consiste à effectuer de manière sécurisée le calcul du couplage entre deux points A et B appartenant à une courbe elliptique, caractérisé en ce qu'il comporte les étapes suivantes :

- 20 1) Génération de deux entiers aléatoires k et k' .
générés aléatoirement entre 0 et $n-1$;
- 2) Calcul des points $P'=k.P$ et $Q'=k'.Q$, où $k.P$ et $k'.Q$ qui dénotent l'opération de multiplication scalaire par les entiers k et k' , respectivement ;
- 25 3) Calcul du couplage $\langle P', Q' \rangle$ entre les points P' et Q' , qui grâce à la propriété de bilinéarité du couplage de point, est égal à $k.k'.\langle P, Q \rangle$;
- 4) Calcul de l'entier $s=1/(k.k') \bmod n$ s'effectuant modulo le nombre de point n du groupe ;
- 30 5) Calcul de l'élément $s.\langle P', Q' \rangle$ à partir des étapes 3 et 4 de manière à obtenir :
 $s.\langle P', Q' \rangle = 1/(k.k') . k.k' . \langle P, Q \rangle = \langle P, Q \rangle$;

6) Retourner $s.\langle P', Q' \rangle = \langle P, Q \rangle$

5 L'avantage du procédé de l'invention est que le calcul du couplage s'effectue sur les points P' et Q' qui sont des points aléatoires. Ainsi, même si un attaquant est capable de mesurer la consommation de courant lors de l'exécution du calcul, il ne peut en déduire aucune information sur les points P et Q .

10 Le procédé de l'invention décrit précédemment permet de protéger le caractère confidentiel des points P et Q mis en œuvre lors de l'exécution du calcul du couplage entre les points P et Q . Il arrive cependant, dans le cadre de certains protocoles cryptographiques,
15 qu'un seul des points P et Q soit confidentiel, l'autre point étant une donnée publique.

Le procédé de la présente invention présente deux variantes de réalisation.

20 Une première variante est tel que le procédé de l'invention, pour lequel le point Q est connu publiquement, est caractérisé en ce qu'il comprend les étapes suivantes :

- 25 1) Génération d'un entier aléatoire k , k étant généré aléatoirement entre 0 et $n-1$;
2) Calcul du point $P' = k.P$;
3) Calcul du couplage $\langle P', Q \rangle$ entre les points P' et Q .
qui, grâce à la propriété de bilinéarité du couplage
30 de point, est égal à $k.\langle P, Q \rangle$;

- 4) Calcul de l'entier $s=1/k \bmod n$ s'effectuant modulo n , calcul s'effectuant modulo le nombre de point n du groupe
- 5) Calcul de l'élément $s.\langle P', Q \rangle$ à partir des étapes 3 et 4 de manière à obtenir :
 $s.\langle P', Q \rangle = (1/k) . k . \langle P, Q \rangle = \langle P, Q \rangle$;
- 6) Retourner $s.\langle P', Q \rangle = \langle P, Q \rangle$

L'avantage de cette première variante du procédé de l'invention est que le calcul du couplage s'effectue sur les points P', Q , le point P' étant aléatoire, et le point Q étant publiquement connu. Ainsi, même si un attaquant est capable de mesurer la consommation de courant lors de l'exécution du calcul, il ne peut en déduire aucune information sur le point P .

La seconde variante du procédé de l'invention décrit précédemment est caractérisé en ce qu'il comporte les étapes suivantes :

20

- 1) Génération d'un point aléatoire R appartenant à la courbe elliptique par la génération d'un entier aléatoire compris entre 0 et $n-1$ et par le calcul de $k.G$, G étant un générateur de la courbe elliptique ;
- 2) Calcul du point $P'=P+R$;
- 3) Calcul des couplages $\langle P', Q \rangle$ et $\langle R, Q \rangle$, qui grâce à la propriété de bilinéarité du couplage de point, est égal à $\langle P', Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle$;
- 4) Calcul de $\langle P, Q \rangle = \langle P', Q \rangle - \langle R, Q \rangle$.

30

L'avantage de cette seconde variante du procédé de l'invention est que le calcul du couplage s'effectue sur les points P' , Q et R , les points P' et R étant aléatoires, et le point Q étant publiquement connu.

5 Ainsi, même si un attaquant est capable de mesurer la consommation de courant lors de l'exécution du calcul, il ne peut en déduire aucune information sur le point P .

La mise en œuvre de l'un quelconque des procédés décrits précédemment permet ainsi la protection d'un

10 module sécurisé ou composant électronique réalisant une opération de couplage de point contre les attaques par mesure de courant. Un exemple de réalisation possible de l'un quelconque desdits procédés décrits précédemment est le suivant : dans le cadre d'un protocole de chiffrement

15 basé sur l'identité, tel que décrit dans la publication : Boneh et Franklin, « Identity-based encryption from the Weil pairing », Proceedings of Crypto 2001 », la clef privée du destinataire du message chiffré est stocké à l'intérieur d'un module sécurisé tel qu'une carte à puce.

20 Lorsque l'utilisateur reçoit un message chiffré, ce message est déchiffré à l'intérieur du module sécurisé. L'intérêt de ce mode de réalisation est que la clef privée reste confinée à l'intérieur du module sécurisé. La mise en œuvre de l'un quelconque desdits procédés

25 décrits précédemment permet alors de protéger l'exécution de l'algorithme de déchiffrement s'effectuant à l'intérieur du module sécurisé, contre les attaques par mesure de courant.

REVENDICATIONS

1. Procédé de contre-mesure dans un composant électronique ou module sécurisé mettant en oeuvre un
- 5 algorithme à clé publique du type courbes elliptiques permettant la protection du calcul de couplage entre deux points A et B appartenant à une courbe elliptique en utilisant la représentation des points de la courbe elliptique en coordonnées projectives consistant à
- 10 représenter un point P ou Q de la courbe elliptique par les coordonnées (X, Y, Z) telles que $x=X/Z$ et $y=Y/Z^3$, x et y étant les coordonnées du point de la courbe elliptique en coordonnées affines, ladite courbe comprenant n éléments et étant définie sur un corps fini
- 15 quelconque, ledit procédé étant caractérisé en ce qu'il comporte les étapes suivantes :
- 1) Génération de deux entiers aléatoires k et k' générés aléatoirement entre 0 et n-1 ;
 - 2) Calcul des points $P'=k.P$ et $Q'=k'.Q$, où k.P et
 - 20 $k'.Q$ qui dénotent l'opération de multiplication scalaire par les entiers k et k', respectivement ;
 - 3) Calcul du couplage $\langle P', Q' \rangle$ entre les points P' et Q', qui grâce à la propriété de bilinéarité du couplage de point, est égal à $k.k'.\langle P, Q \rangle$;
 - 25 4) Calcul de l'entier $s=1/(k.k') \bmod n$ s'effectuant modulo le nombre de point n du groupe ;
 - 5) Calcul de l'élément $s.\langle P', Q' \rangle$ à partir des étapes 3 et 4 de manière à obtenir : $s.\langle P', Q' \rangle = 1/(k.k') . k.k' . \langle P, Q \rangle = \langle P, Q \rangle$;
 - 30 6) Obtention du résultat tel que : $s.\langle P', Q' \rangle = \langle P, Q \rangle$.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte les étapes suivantes :

- 1) Génération d'un entier aléatoire k , k étant
5 généré aléatoirement entre 0 et $n-1$;
- 2) Calcul du point $P' = k.P$;
- 3) Calcul du couplage $\langle P', Q \rangle$ entre les points P' et Q . qui, grâce à la propriété de bilinéarité du couplage de point, est égal à $k.\langle P, Q \rangle$;
- 10 4) Calcul de l'entier $s = 1/k \bmod n$ s'effectuant modulo n , calcul s'effectuant modulo le nombre de point n du groupe ;
- 5) Calcul de l'élément $s.\langle P', Q \rangle$ à partir des étapes 3 et 4 de manière à obtenir :
- 15 $s.\langle P', Q \rangle = (1/k).k.\langle P, Q \rangle = \langle P, Q \rangle$;
- 6) Obtention du résultat tel que : $s.\langle P', Q \rangle = \langle P, Q \rangle$

3. Procédé selon la revendication 2, caractérisé en ce qu'il comporte les étapes suivantes :

- 20 1) Génération d'un point aléatoire R appartenant à la courbe elliptique par la génération d'un entier aléatoire compris entre 0 et $n-1$ et par le calcul de $k.G$, G étant un générateur de la courbe elliptique ;
- 25 2) Calcul du point $P' = P + R$;
- 3) Calcul des couplages $\langle P', Q \rangle$ et $\langle R, Q \rangle$, qui grâce à la propriété de bi-linéarité du couplage de point, est égal à $\langle P', Q \rangle = \langle P, Q \rangle + \langle R, Q \rangle$;
- 4) Calcul de $\langle P, Q \rangle = \langle P', Q \rangle - \langle R, Q \rangle$.

30

4. Procédé selon la revendication 3, dans lequel la première étape est réalisée en générant un entier

aléatoire compris entre 0 et $n-1$, et en calculant le point $k.G$, G étant un générateur de la courbe elliptique.

5 5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le procédé de calcul s'effectue sur une carte à puce.

6. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que le calcul s'effectue sur un module TPM pour « Trusted Platform Module » installé dans un PC non sécurisé.

10 7. Composant électronique caractérisé en ce qu'il met oeuvre le procédé de contre-mesure selon l'une quelconque des revendications précédentes.

8. Composant électronique selon la revendication 7 caractérisé en ce qu'il consiste en une carte à puce.

15 9. Composant électronique selon la revendication 7 caractérisé en ce qu'il consiste en un module TPM pour « Trusted Platform Module » installé dans un PC non sécurisé.