

(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
26 février 2004 (26.02.2004)

PCT

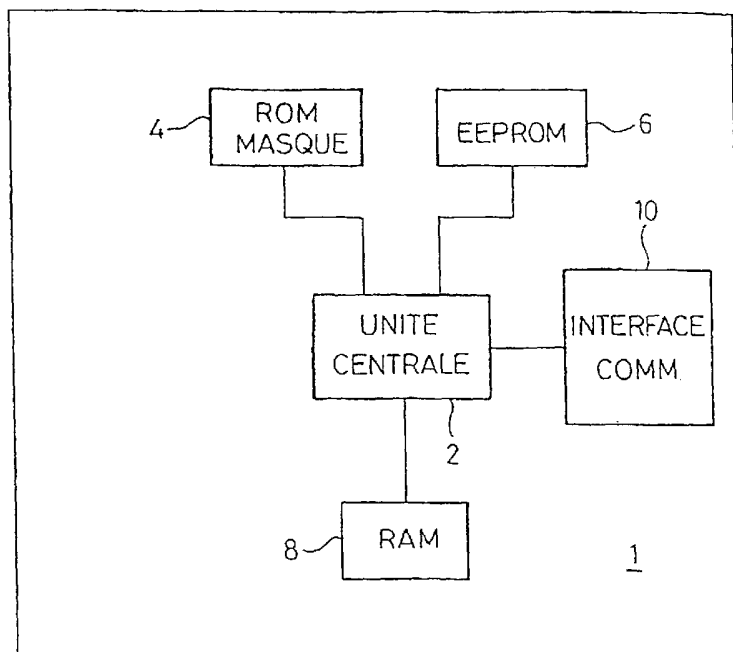
(10) Numéro de publication internationale
WO 2004/017193 A2

- (51) Classification internationale des brevets⁷ : **G06F 7/72** (72) Inventeurs; et
(21) Numéro de la demande internationale : PCT/FR2003/002462 (75) Inventeurs/Déposants (pour US seulement) : **BILLET, Olivier** [FR/FR]; 1211, route des Vallettes Sud, F-06140 Tourrettes sur Loup (FR). **JOYE, Marc** [FR/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).
(22) Date de dépôt international : 5 août 2003 (05.08.2003)
(25) Langue de dépôt : français (74) Mandataire : **BRUYERE, Pierre**; Gemplus, Service Brevets, La Vigie, Boîte postale 90, F-13705 La Ciotat Cedex (FR).
(26) Langue de publication : français
(30) Données relatives à la priorité : 02/10193 9 août 2002 (09.08.2002) FR (81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
(71) Déposant (pour tous les États désignés sauf US) : **GEM-PLUS** [FR/FR]; Département Brevets, La Vigie, Boîte postale 90, F-13705 La Ciotat Cedex (FR).

[Suite sur la page suivante]

(54) Title: METHOD FOR UNIVERSAL CALCULATION APPLIED TO POINTS OF AN ELLIPTIC CURVE DEFINED BY A QUARTIC, RELATED CRYPTOGRAPHIC METHOD AND ELECTRONIC COMPONENT

(54) Titre : PROCEDE DE CALCUL UNIVERSEL APPLIQUE A DES POINTS D'UNE COURBE ELLIPTIQUE DEFINIE PAR UNE QUARTIQUE, PROCEDE CRYPTOGRAPHIQUE ET COMPOSANT ELECTRONIQUE ASSOCIES



2...CENTRAL UNIT
4...MASK ROM
6...EEPROM
8...RAM
10...COMMUNICATION INTERFACE

(57) Abstract: The invention concerns a method for universal calculation on the points of an elliptic curve. The invention is characterized in that the elliptic curve is defined by a quartic equation and identical programmed calculating means are used for operating an addition of points, a doubling of points and an addition of a neutral point, the calculating means comprising in particular a central unit (2) associated with a memory (4, 6, 8). The invention also concerns a cryptographic method using such a universal method. The invention further concerns a component for implementing the universal calculation method and/or the cryptographic method. For example, the invention is applicable to smart cards.

[Suite sur la page suivante]



MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

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

Déclarations en vertu de la règle 4.17 :

- relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)
- relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations

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.

(57) **Abstré :** L'invention concerne un procédé de calcul universel sur des points d'une courbe elliptique. Selon l'invention, la courbe elliptique est définie par une équation quartique et des moyens de calcul programmés identiques sont utilisés pour réaliser une opération d'addition de points, une opération de doublement de points, et une opération d'addition d'un point neutre, les moyens de calcul comprenant notamment une unité centrale (2) associée à une mémoire (4, 6, 8). L'invention concerne également un procédé cryptographique utilisant un tel procédé universel. L'invention concerne encore un composant pour mettre en œuvre le procédé de calcul universel et / ou le procédé cryptographique. Exemple d'application: cartes à puce.

**PROCEDE DE CALCUL UNIVERSEL APPLIQUE A DES POINTS D'UNE
COURBE ELLIPTIQUE DEFINIE PAR UNE QUARTIQUE, PROCEDE
CRYPTOGRAPHIQUE ET COMPOSANT ELECTRONIQUE ASSOCIES**

La présente invention concerne un procédé de calcul universel appliqué à des points d'une courbe elliptique, et un composant électronique comprenant des moyens de mise en œuvre d'un tel procédé. L'invention est notamment
5 applicable pour la mise en œuvre d'algorithmes cryptographiques du type à clé publique, par exemple dans des cartes à puce.

Les algorithmes à clé publique sur courbe elliptique permettent des applications cryptographiques
10 de type chiffrement, signature numérique, authentification...

Ils sont notamment très utilisés dans des applications de type carte à puce, parce qu'ils permettent d'utiliser des clés de faible longueur,
15 autorisant des temps de traitement assez courts, et qu'ils peuvent ne pas nécessiter l'utilisation de crypto-processeurs pour leur implémentation, ce qui diminue le prix de revient des composants électroniques dans lesquels ils sont implémentés.

20 Avant d'aller plus loin, il convient tout d'abord de faire quelques rappels sur les courbes elliptiques.

Les points d'une courbe elliptique sont définis sur un corps K et forment un groupe abélien $E(K)$, dans lequel
25 l'opération de groupe est l'addition de points notée $+$, et où il se distingue un élément neutre noté O .

Pour un corps fini, le cardinal de $E(K)$ est fini. Il existe donc pour tout point P un entier m tel que :

$$O = m.P = P + P + \dots + P, \text{ m fois}$$

et tel que pour tout entier $k < m$, on a $k.P \neq O$. Un tel entier m est appelé ordre de P . Dans ce cas, m divise le cardinal de $E(K)$.

Certaines courbes ont des propriétés particulières. Par exemple, une courbe elliptique ayant un point d'ordre 2 a un cardinal divisible par 2. Ou bien, une courbe elliptique ayant un point d'ordre trois est une courbe telle que le cardinal du groupe $E(K)$ est divisible par 3. Les courbes ayant une même propriété particulière sont regroupées dans une même famille.

Un point d'une courbe elliptique peut être représenté par plusieurs types de coordonnées, par exemple par des coordonnées affines ou des coordonnées projectives de Jacobi.

Il existe différents modèles pour définir une courbe elliptique applicable en cryptographie. Un modèle couramment utilisé est le modèle dit de Weierstrass. Le modèle de Weierstrass est très général puisque toute courbe elliptique peut se ramener sous ce modèle.

Chaque modèle peut être utilisé à l'aide des différents types de coordonnées.

Par exemple, en coordonnées affines et dans le cas où la caractéristique p du corps K est différente de 2 et 3, le modèle de Weierstrass est défini de la manière suivante : le point neutre O (le point à l'infini dans le modèle de Weierstrass) et l'ensemble des points $(X, Y) \in K \times K$, vérifiant l'équation :

$$E/K : Y^2 = X^3 + aX + b \quad (F1)$$

avec $a, b \in K$ tels que $4a^3 + 27b^2 \neq 0$, forment le groupe des points rationnels d'une courbe elliptique $E(K)$. Le point P peut aussi être représenté par des coordonnées projectives de Jacobi de la forme générale (U, V, W) . (X, Y) et (U, V, W) sont liées par les relations suivantes :

$$X = U/W \quad \text{et} \quad Y = V/W^2 \quad (F2)$$

Avec ces coordonnées projectives de Jacobi, l'équation de Weierstrass d'une courbe elliptique devient :

$$E/K : V^2 = U^3 + a*UW^4 + b*W^6 \quad (F3)$$

5 Les coordonnées projectives sont notamment intéressantes dans les calculs d'exponentiation appliqués à des points d'une courbe elliptique, car ils ne comportent pas de calculs d'inversion dans le corps.

Comme le montrent la formule F2, un même point a
10 plusieurs représentations possibles en coordonnées projectives de Jacobi. Aussi, on définit sur $K^3 \setminus \{(0, 0, 0)\}$, la relation d'équivalence suivante : deux éléments, de coordonnées (U, V, W) et (U', V', W') sont dits équivalents et appartiennent à une même classe
15 d'équivalence si et seulement si il existe un élément λ non nul de K tel que

$$(U', V', W') = (\lambda U, \lambda^2 V, \lambda W) \quad (F4)$$

Les coordonnées d'un l'élément de cette classe sont notées $(U : V : W)$.

20

Selon le modèle qui définit la courbe elliptique et selon les coordonnées avec lesquelles on travaille, différentes formules d'addition, de soustraction et de doublement de points sont applicables. Dans le cas du
25 modèle de Weierstrass, de telles formules sont connues et données par la règle bien connue de la sécante et de la tangente.

Dans l'exemple d'une courbe elliptique E donnée par un modèle de Weierstrass en coordonnées affines sur un
30 corps de caractéristique différente de 2 et 3, les formules d'addition, de soustraction et de doublement de points les plus simples sont les suivantes.

L'inverse d'un point $P_1 = (X_1, Y_1)$ de la courbe E est le point $-P_1 = (X_1, \bar{Y}_1)$ avec

$$35 \quad \bar{Y}_1 = -Y_1 \quad (F5)$$

L'opération d'addition des points P1 de coordonnées (X1, Y1) et P2 de coordonnées (X2, Y2) de cette courbe, avec $P1 \neq -P2$, donne le point $P3 = P1 + P2$ dont les coordonnées (X3, Y3) sont telles que :

$$5 \quad X3 = \lambda^2 - X1 - X2 \quad (F6)$$

$$Y3 = \lambda \times (X1 - X3) - Y1, \quad (F7)$$

avec

$$\lambda = (Y1 - Y2) / (X1 - X2), \text{ si } P1 \neq P2 \quad (F8)$$

$$\lambda = (3 \times X1^2 + a) / (2 \times Y1), \text{ si } P1 = P2 \quad (F9)$$

10 La formule F8 est utilisée pour additionner deux points distincts ($P3 = P1 + P2$) tandis que la formule F9 est utilisée pour une opération de doublement de point ($P3 = 2 \times P1$).

Les formules F6 à F9 ne sont pas valables lorsque
 15 P1 et / ou P2 est égal au point neutre O. Le plus souvent, en pratique, on ne réalise pas d'opération de type $P3 = P1 + O$. Plus simplement, avant la réalisation d'une opération d'addition de type $P3 = P1 + P2$, il est testé si l'un au moins des points est égal au neutre O.
 20 On réalise alors l'opération $P3 = P1$ si $P1 = O$ ou $P3 = P2$ si $P2 = O$.

Les opérations d'addition ou soustraction, de doublement d'un point et l'opération d'addition du neutre sont les opérations de base utilisées dans les
 25 algorithmes de multiplication scalaire sur les courbes elliptiques : étant donné un point P1 appartenant à une courbe elliptique E et d un nombre prédéterminé (un entier), le résultat de la multiplication scalaire du point P1 par le nombre d est un point P2 de la courbe E tel que $P2 = d \times P1 = P1 + P1 + \dots + P1$, d fois. A noter que si P1 est d'ordre n, alors $n \times P1 = O$,
 30 $(n+1) \times P1 = P1 + O = P1$ etc., O étant le point neutre.

Les algorithmes cryptographiques à clé publique sur courbe elliptique sont basés sur la multiplication
 35 scalaire d'un point P1 sélectionné sur la courbe, par un nombre prédéterminé d, une clé secrète. Le résultat de

cette multiplication scalaire $d \times P_1$ est un point P_2 de la courbe elliptique. Dans un exemple d'application au chiffrement selon le procédé de El Gamal, le point P_2 obtenu est la clé publique qui sert au chiffrement d'un message.

Le calcul de la multiplication scalaire $P_2 = d \times P_1$ peut être réalisé par différents algorithmes. On peut en citer quelques-uns, comme l'algorithme de doublement et d'addition ("double and add" dans la littérature anglo-saxonne) basé sur la représentation binaire du multiplieur d , l'algorithme dit "d'addition-soustraction" basé sur la représentation binaire signée du multiplieur d , l'algorithme avec fenêtre...

Tous ces algorithmes utilisent les formules d'addition, de soustraction, de doublement et d'addition du neutre définies sur les courbes elliptiques.

Cependant, ces algorithmes se révèlent sensibles aux attaques visant à découvrir notamment la valeur de la clé secrète d . On peut citer notamment les attaques à canaux cachés, simples ou différentielles.

On entend par attaque à canal caché simple ou différentielle, une attaque basée sur une grandeur physique mesurable de l'extérieur du dispositif, et dont l'analyse directe (attaque simple) ou l'analyse selon une méthode statistique (attaque différentielle) permet de découvrir des informations contenues et manipulées dans des traitements dans le dispositif. Ces attaques peuvent ainsi permettre de découvrir des informations confidentielles. Ces attaques ont notamment été dévoilées dans D1 (Paul Kocher, Joshua JAFFE et Benjamin JUN. Differential Power Analysis. Advances in Cryptology - CRYPTO'99, vol. 1666 of Lecture Notes in Computer Science, pp.388-397. Springer-Verlag, 1999). Parmi les grandeurs physiques qui peuvent être exploitées à ces fins, on peut citer le temps d'exécution, la consommation en courant, le champ électromagnétique rayonné par la

partie du composant utilisée pour exécuter le calcul, etc. Ces attaques sont basées sur le fait que la manipulation d'un bit, c'est à dire son traitement par une instruction particulière, a une empreinte particulière sur la grandeur physique considérée selon la valeur de ce bit et/ou selon l'instruction.

Dans les systèmes cryptographiques basés sur des courbes elliptiques, ces attaques visent à identifier une opération (par exemple une addition de points de type $P_3 = P_1 + P_2$, une addition de type $P_3 = P_1 + O$, une multiplication scalaire de type $P_3 = d \cdot P_1$) dans un ensemble d'opérations réalisées successivement.

Si on prend l'exemple d'un algorithme de multiplication scalaire sur courbes elliptiques avec le modèle de Weierstrass, cet algorithme peut être sensible aux attaques à canaux cachés de type simple, car les opérations de base de doublement de points, d'addition de points ou d'addition du point neutre sont sensiblement différentes comme le montre le calcul du lambda dans les formules F8 et F9 supra.

Il est donc nécessaire de prévoir des procédés de contre-mesure permettant d'empêcher les différentes attaques de prospérer. En d'autres termes, il est nécessaire de sécuriser les algorithmes de multiplication scalaire.

Pour cela, de D2 (Eric Brier et Marc Joye. Weierstrass elliptic curves and side-channel attacks. In D. Naccache, editor, Public Key Cryptography, volume 2274 of Lecture Notes in Computer Science, pages 335-345. Springer-Verlag, 2002), il est connu une formulation unique pour une opération de doublement de points et une opération d'addition de points. Ainsi, les deux opérations ne peuvent plus être différenciées par une attaque à canal caché. Cette formulation cependant

présente l'inconvénient de ne pas être valable pour réaliser une opération d'addition du point neutre.

De D3 (Pierre-Yvan Liardet et Nigel P. Smart. Preventing SPA/DPA in ECC systems using the Jacobi form. In C.K.Koç, D. Naccache, and C. Paar, editors, Cryptographic Hardware and embedded Systems - CHES 2001, volume 2162 of Lecture Notes in Computer Science, pages 391-401. Springer-Verlag, 2001), il est également connu une formulation unique pour une opération d'addition et
10 une opération de doublement de points. Cette formulation cependant n'est applicable que dans le cadre d'une courbe elliptique ayant trois points d'ordre 2. De plus, la formulation proposée dans D3 demande un espace mémoire considérable pour être mise en œuvre car les points sont
15 mémorisés avec quatre coordonnées. Ceci est difficilement compatible avec une application de type carte à puce.

De D4 (Marc Joye et Jean-Jacques Quisquater. Hessian elliptic curves and side-channel attacks. In C.K.Koç, D. Naccache, and C. Paar, editors, Cryptographic
20 Hardware and embedded Systems - CHES 2001, volume 2162 of Lecture Notes in Computer Science, pages 402-410. Springer-Verlag, 2001), il est encore connu une formulation unique pour une opération d'addition et une opération de doublement de points. Cependant, cette
25 formulation est applicable uniquement aux courbes elliptiques ayant un point d'ordre trois.

D3 et D4 n'évoquent pas le problème de l'addition du neutre.

30 Un but de l'invention est de proposer une solution de protection contre les attaques à canaux cachés, notamment les attaques SPA, plus efficace que les solutions déjà connues.

Un autre but de l'invention est de proposer une
35 solution qui peut être mise en œuvre dans un circuit

disposant de peu d'espace mémoire, en vue par exemple d'une application de type carte à puce.

Ces objectifs sont atteints dans l'invention par une formulation unique permettant de réaliser une
5 addition de deux points distincts, un doublement de points, et une opération d'addition du neutre. La dite formulation selon l'invention est de plus minimale : on limite ainsi le nombre d'opérations à effectuer et l'espace mémoire nécessaire pour sa mise en œuvre.

10

Ainsi, l'invention concerne un procédé de calcul universel sur des points d'une courbe elliptique. Selon l'invention, la courbe elliptique est définie par une équation quartique et des moyens de calcul programmés
15 identiques sont utilisés pour réaliser une opération d'addition de points, une opération de doublement de points, et une opération d'addition d'un point neutre, les moyens de calcul comprenant notamment une unité centrale associée à une mémoire.

20

En d'autres termes, selon l'invention, l'utilisation d'un modèle de la courbe elliptique sous forme de quartique (c'est-à-dire d'un polynôme du 4^{ème} degré) permet d'utiliser une formulation unique pour réaliser des opérations d'addition de points, de
25 doublement de point et de d'addition du point neutre de la courbe.

Il devient alors impossible de distinguer l'une de ces opérations des autres par une attaque telle qu'une attaque à canal caché.

30

Par ailleurs, l'utilisation d'un modèle de la courbe sous forme de quartique permet de représenter un point à l'aide de seulement 3 coordonnées projectives, ce qui limite l'espace mémoire nécessaire pour mémoriser les coordonnées d'un point et diminue les temps de calcul
35 lors d'opérations sur des points.

Enfin, comme on le verra mieux dans des exemples, la formulation unique obtenue selon l'invention pour réaliser trois types d'addition (addition de deux points distincts, doublement de points et addition du neutre) utilise un nombre limité d'opérations élémentaires de type multiplication, ce qui limite encore les temps de calcul et l'espace mémoire nécessaire.

L'invention concerne également l'utilisation d'un procédé de calcul universel tel que décrit ci-dessus, dans un procédé de calcul de multiplication scalaire appliqué à des points d'une courbe elliptique, et / ou dans un procédé cryptographique.

L'invention concerne encore un composant électronique comprenant des moyens de calcul programmés pour mettre en œuvre un procédé de calcul universel tel que décrit ci-dessus ou un procédé cryptographique utilisant le procédé de calcul universel ci-dessus. Les moyens de calcul comprennent notamment une unité centrale associée à une mémoire.

Enfin, l'invention concerne également une carte à puce comprenant le composant électronique ci-dessus.

L'invention et les avantages qui en découlent apparaîtront plus clairement à la lecture de la description qui suit d'exemples particuliers de réalisation de l'invention, donnés à titre purement indicatif et en référence à la figure unique en annexe. Celle-ci représente sous forme de schéma bloc un dispositif 1 électronique apte à réaliser des calculs cryptographiques.

Dans les exemples suivants, le dispositif 1 est une carte à puce destinée à exécuter un programme cryptographique. A cette fin, le dispositif 1 réunit dans une puce des moyens de calcul programmés, composés d'une

unité centrale 2 reliée fonctionnellement à un ensemble de mémoires dont :

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

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

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

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

Pour réaliser ces fonctions, l'unité centrale 2 exécute un algorithme cryptographique sur des données de

programmation qui sont stockées dans les parties ROM masque 4 et/ou EEPROM 6.

L'algorithme utilisé ici est un algorithme à clé publique sur courbe elliptique dans le cadre d'un modèle sous forme d'une quartique. On s'intéressera plus précisément ici à une partie de cet algorithme, qui permet de réaliser des opérations de base, c'est-à-dire des opérations d'addition : addition de deux points distincts, de deux points identiques (c'est-à-dire une opération de doublement d'un point), de un point quelconque et du point neutre.

On rappelle que, selon l'invention, ces trois opérations sont réalisées à partir de la même formulation et sont donc non distinguables l'une de l'autre depuis l'extérieur pour une attaque à canal caché simple.

Dans le cadre de l'invention, on s'intéresse aux modèles de courbes elliptiques définies par une équation quartique au lieu de l'équation cubique de Weierstrass habituellement utilisée.

La forme générale d'une quartique, en coordonnées affines, est donnée par la relation :

$$Y^2 = a_0.X^4 + a_1.X^3 + a_2.X^2 + a_3.X + a_4 \quad (F10)$$

ou, en coordonnées projectives de Jacobi par la relation :

$$V^2 = a_0.U^4 + a_1.U^3W + a_2.U^2W^2 + a_3.UW^3 + a_4.W^4 \quad (F11)$$

sachant que les coordonnées affines et les coordonnées projective de Jacobi d'un même point sont liées par la relation :

$$(X, Y) = (U/W, V/W^2) \quad (F12)$$

Dans un premier exemple de mise en œuvre de l'invention, on considère une courbe elliptique quelconque, et on réalise une opération de type $P_3 = P_1 + P_2$, avec P_1, P_2 , deux points quelconques de la courbe elliptique. P_2 peut être différent de P_1 , égal à P_1 et /

ou égal au neutre O de la courbe. L'opération d'addition est réalisée en coordonnées projectives de Jacobi.

On montre que toute courbe d'équation

$$Y^2 = X^3 + a.X + b \text{ (équation de Weierstrass)}$$

5 est birationnellement équivalente à une courbe d'équation

$$Y^2 = b.X^4 + a.X^3 + X \quad (F13)$$

L'équation F13 est finalement un cas particulier de l'équation F10, avec $a_0=b$, $a_1=a$, $a_2=0$, $a_3=1$, $a_4=0$.

10 En utilisant les relations d'équivalence F12, on montre que l'équation F13 peut également s'écrire, en coordonnées projectives de Jacobi :

$$V^2 = b.U^4 + a.U^3W + UW^3 \quad (F14)$$

15 Lorsque le dispositif de calcul de multiplication scalaire est sollicité pour réaliser une opération d'addition, l'unité centrale 2 mémorise tout d'abord dans des registres de calcul les coordonnées $(U1 : V1 : W1)$ et $(U2 : V2 : W2)$ des points $P1$, $P2$ de la courbe elliptique, à additionner.

20 L'unité centrale 2 calcule ensuite les coordonnées du point $P3$ selon les relations :

$$U3 = 2.b.U1^2.U2^2 + (aU1.U2 + W1.W2).(U1.W2+W1.U2) + 2V1.V2 \quad (F15)$$

$$\begin{aligned} V3 = & (U1^2.V2+U2^2.V1) * \\ & (4b.(U1.W2+U2.W1).W1.W2 \\ & - 8b^2.(U1.U2)^2 \\ & + a.[(2W1.W2)^2 - (aU1.U2+W1.W2)^2] \\ & + (W1^2.V2+W2^2.V1) * \\ & [(aU1.U2+W1.W2)^2 - (2aU1.U2)^2 + 4bU1.U2.(W1.U2+U1.W2)] \\ & - 4bU1.U2.(U1.W1.V2+U2.W2.V1)(aU1.U2-W1.W2) \end{aligned} \quad (F16)$$

$$W3 = (aU1.U2-W1.W2)^2 - 4bU1.U2(U1.W2+U2.W1) \quad (F17)$$

35 Les coordonnées $(U3 : V3 : W3)$ du point $P3$ sont finalement mémorisées dans des registres de la mémoire de travail 8, pour être utilisées par ailleurs, par exemple pour la suite de l'algorithme de chiffrement.

On vérifie que les formules F15 à F17 sont valides, même dans le cas où $P1 = P2$ (doublement de point) ou dans le cas où $P2 = O(0 : 0 : 1)$ (addition du neutre).

5 Dans un deuxième exemple de mise en œuvre de l'invention, on considère une courbe elliptique ayant un seul point d'ordre deux, de coordonnées affines $(\theta, 0)$, et on réalise une opération de type $P3 = P1 + P2$, avec $P1, P2$, deux points quelconques de la courbe elliptique. $P2$ peut
10 être différent de $P1$, égal à $P1$ et / ou égal au neutre O de la courbe. L'opération d'addition est donnée en coordonnées projectives de Jacobi.

Le point d'ordre deux vérifiant l'équation de Weierstrass définissant la courbe elliptique, θ est défini
15 par la relation :

$$\theta^3 + a.\theta + b = 0$$

On montre alors que toute courbe d'équation

$$Y^2 = X^3 + a.X + b \text{ (équation de Weierstrass)}$$

et ayant un unique point $(\theta, 0)$ d'ordre deux est
20 birationnellement équivalente à une courbe d'équation

$$Y^2 = \varepsilon.X^4 - 2\delta.X^2 + 1 \quad (F18)$$

avec :

$$\varepsilon = - (a+3\theta^2/4)/4 \quad \text{et} \quad \delta = 3\theta/4 \quad (F19)$$

L'équation F18 est finalement un cas particulier de
25 l'équation F10, avec $a0=\varepsilon, a1=0, a2=-2\delta, a3=0, a4=1$.

En utilisant les relations d'équivalence F12, on montre que l'équation F18 peut également s'écrire, en coordonnées projectives de Jacobi :

$$V^2 = \varepsilon.X^4 - 2\delta.U^2X^2 + W^4 \quad (F20)$$

30 Le passage du modèle cubique $Y^2 = X^3 + aX + b$ au modèle quartique $Y^2 = \varepsilon.X^4 - 2\delta.X^2 + 1$ se fait par les transformations suivantes :

	modèle de Weierstrass		modèle quartique
35	$(\theta, 0)$	ξ	$(0 : -1 : 1)$
	(X, Y)	ξ	$(2(X-\theta) : (2X+\theta)(X-\theta)^2 - Y^2 : Y)$

$O \quad \xi \quad (0 : 1 : 1)$
 modèle modèle de
 quartique Weierstrass
 $(0 : 1 : 1) \xi O$
 5 $(0 : -1 : 1) \xi (\theta, 0)$
 $(U : V : W) \xi (2(V+W^2)/U^2 - \theta/2, W(4V+4W^2-3\theta U^2)U^3)$
 On définit pour ce modèle quartique le point neutre
 $O (0 : 1 : 1)$ et le point inverse du point $P (U : V : W)$
 par le point $-P (-U : V : W)$.
 10 Lorsque le dispositif de calcul d'exponentiation
 est sollicité pour réaliser une opération d'addition,
 l'unité centrale 2 mémorise tout d'abord dans des
 registres de calcul les coordonnées $(U1 : V1 : W1)$ et
 $(U2 : V2 : W2)$ des points $P1, P2$ de la courbe elliptique,
 15 à additionner.
 L'unité centrale 2 calcule ensuite les coordonnées
 du point $P3$ selon les relations :
 $U3 = U1.W1.V2 + V1.U2.W2 \quad (F21)$
 $V3 = [(W1.W2)^2 + \varepsilon(U1.U2)^2]$
 20 $* [V1.V2 - 2\delta U1.U2.W1.W2] + 2\varepsilon.U1.U2.W1.W2 (U1^2 W2^2 + W1^2 U2^2) \quad (F22)$
 $W3 = (W1.W2)^2 - \varepsilon(U1.U2)^2 \quad (F23)$
 Les coordonnées $(U3 : V3 : W3)$ du point $P3$ sont
 finalement mémorisées dans des registres de la mémoire de
 travail 8, pour être utilisées par ailleurs, par exemple
 25 pour la suite de l'algorithme de chiffrement.
 On vérifie là encore que les formules $F21$ à $F23$
 sont valides, même dans le cas où $P1 = P2$ (doublement de
 point) ou dans le cas où $P2 = O$ (addition du neutre).
 30 Dans un troisième exemple de mise en œuvre de
 l'invention, on considère un cas particulier du deuxième
 exemple, dans lequel la courbe elliptique a trois points
 d'ordre deux et est telle que $\varepsilon = 1$. Egalement, on réalise
 une opération de type $P3 = P1 + P2$, avec $P1, P2$, deux
 35 points quelconques de la courbe elliptique. $P2$ peut être
 différent de $P1$, égal à $P1$ et / ou égal au neutre O de la

courbe. L'opération d'addition est donnée en coordonnées projectives de Jacobi pour le modèle $U^4 - 2\delta.U^2.W^2 + W^4$ correspondant au modèle affine $Y^2 = X^4 + 2\delta.X^2 + 1$.

5 L'équation F24 est finalement un cas particulier de l'équation F10 la plus générale, avec $a_0 = 1$, $a_1 = 0$, $a_2 = -2\delta$, $a_3 = 0$, $a_4 = 1$.

10 Lorsque le dispositif de calcul d'exponentiation est sollicité pour réaliser une opération d'addition, l'unité centrale 2 mémorise tout d'abord dans des registres de calcul les coordonnées $(U_1 : V_1 : W_1)$ et $(U_2 : V_2 : W_2)$ des points P_1 , P_2 de la courbe elliptique, à additionner.

15 L'unité centrale 2 calcule ensuite les coordonnées du point P_3 selon les relations :

$$U_3 = U_1.W_1.V_2 + V_1.U_2.W_2 \quad (F27)$$

$$V_3 = [(W_1.W_2)^2 + (U_1.U_2)^2]$$

$$* [V_1.V_2 - 2\delta.U_1.U_2.W_1.W_2] + 2U_1.U_2.W_1.W_2 (U_1^2.W_2^2 + W_1^2.U_2^2) \quad (F28)$$

20 $W_3 = (W_1.W_2)^2 - (U_1.U_2)^2 \quad (F29)$

Les coordonnées $(U_3 : V_3 : W_3)$ du point P_3 sont finalement mémorisées dans des registres de la mémoire de travail 8, pour être utilisées par ailleurs, par exemple pour la suite de l'algorithme de chiffrement.

25 On vérifie là encore que les formules F27 à F29 sont efficaces, même dans le cas où $P_1 = P_2$ (doublement de point) ou dans le cas où $P_2 = O$ (addition du neutre).

30 D'un point de vue réalisation pratique, les formules F27 à F29 peuvent être réalisées de la manière suivante :

$$r_1 \leftarrow u_1.u_2$$

$$r_2 \leftarrow w_1.w_2$$

$$r_3 \leftarrow r_1.r_2$$

35 $r_4 \leftarrow v_1.v_2$

$$r_5 \leftarrow u_1.w_1 + v_1$$

```

r6 p u2.w2 + v2
u3 p r5.r6 - r4-r3
w3 p (r2-r1).(r2+r1)
r6 p δ*r3
5   r4 p r4 - 2.r6
    r6 p (r2+r1)2-2r3
    r4 p r4.r6
    r6 p (u1+w1).(u2+w2)-r1-r2
    r5 p r62 - 2r3
10  r6 p r5.r3
    v3 p r4 + 2.r6

```

où u1, v1, w1, u2, v2, w2, u3, v3, w3 sont des registres de calcul dans lesquels sont mémorisées les coordonnées projectives des points P1, P2, P3, et r1 à r6 sont des registres temporaires de calcul.

Ainsi, selon ce mode de réalisation, les coordonnées du point P3 sont obtenues en un temps égal approximativement à 13 fois le temps de réalisation d'une multiplication du contenu de deux registres + une fois le temps de réalisation d'une multiplication du contenu d'un registre par une constante. Le temps de calcul des coordonnées de P3 à l'aide de la formulation selon l'invention est ainsi bien inférieur au temps de calcul des coordonnées de P3 à l'aide d'une formulation telle que celles de l'art antérieur.

A noter que cette approximation est tout à fait réaliste car le temps de réalisation d'une multiplication du contenu d'un registre par une constante ou d'une multiplication du contenu de deux registres est en pratique très supérieur au temps de réalisation d'une addition du contenu de deux registres.

Ceci est également vrai dans le cas de la mise en œuvre des formules F15-F17 ou F21-F23.

Dans un quatrième exemple de mise en œuvre de l'invention, on considère une courbe elliptique ayant un

seul point d'ordre deux, de coordonnées affines $(0, 0)$, et on réalise une opération de type $P3 = P1+P2$, avec $P1, P2$, deux points quelconques de la courbe elliptique. $P2$ peut être différent de $P1$, égal à $P1$ et / ou égal au neutre O de la courbe.

Comme on l'a vu dans le deuxième exemple :

$$\theta^3 + a.\theta + b = 0$$

La courbe d'équation de Weierstrass

$$Y^2 = X^3 + a.X + b$$

et ayant un unique point $(0, 0)$ d'ordre deux est birationnellement équivalente à une courbe d'équation

$$Y^2 = \varepsilon.X^4 - 2\delta.X^2 + 1 \quad (F18)$$

avec :

$$\varepsilon = -(a+3\theta^2/4)/4 \quad \text{et} \quad \delta = 3\theta/4 \quad (F19)$$

L'opération d'addition est donnée dans cet exemple en coordonnées affines.

Lorsque le dispositif de calcul d'exponentiation est sollicité pour réaliser une opération d'addition, l'unité centrale 2 mémorise tout d'abord dans des registres de calcul les coordonnées $(X1, Y1)$ et $(X2, Y2)$ des points $P1, P2$ de la courbe elliptique, à additionner.

L'unité centrale 2 calcule ensuite les coordonnées du point $P3$ selon les relations :

$$X3 = (X1.Y2 + Y1.X2) / [1 - \varepsilon(X1.X2)^2] \quad (F30)$$

$$Y3 = \{ [1+\varepsilon(X1.X2)^2] . [Y1.Y2 - 2\delta.X1.X2] + 2\varepsilon.X1.X2.(X1^2+X2^2) \} / [1 - \varepsilon(X1.X2)^2] \quad (F31)$$

Les coordonnées $(X3, Y3)$ du point $P3$ sont finalement mémorisées dans des registres de la mémoire de travail 8, pour être utilisées par ailleurs, par exemple pour la suite de l'algorithme de chiffrement.

On vérifie là encore que les formules F30 à F31 sont valides, même dans le cas où $P1 = P2$ (doublement de point) ou dans le cas où $P2 = O$ (addition du neutre).

REVENDICATIONS

1. Procédé de calcul universel sur des points d'une courbe elliptique, caractérisé en ce que la courbe elliptique est définie par une équation quartique et en ce que des moyens de calcul programmés identiques sont
5 utilisés pour réaliser une opération d'addition de points, une opération de doublement de points, et une opération d'addition d'un point neutre, les moyens de calcul comprenant notamment une unité centrale (2) associée à une mémoire (4, 6, 8).

10

2. Procédé selon la revendication 1, caractérisé en ce que la courbe elliptique est définie par une équation quartique de type :

$$V^2 = b.U^4 + a.U^3.W + U.W^3,$$

15

(U : V : W) étant des coordonnées projectives de Jacobi d'un point P de la courbe elliptique, et a, b étant des paramètres de la courbe elliptique, un point de coordonnées (0 : 0 : 1) étant un point neutre O de la courbe elliptique, un point de coordonnées (U : -V : W)
20 étant un point inverse (-P) du point P de coordonnées (U : V : W).

3. Procédé selon la revendication 2, dans lequel le point P est également défini en coordonnées affines
25 (X, Y), les coordonnées affines (X, Y) et les coordonnées projectives de Jacobi (U : V : W) du point P étant liées par les relations :

$$(X, Y) = (U/W, V/W^2).$$

30

4. Procédé selon la revendication 2 ou 3, dans lequel, pour réaliser l'addition d'un premier point P1 défini par des premières coordonnées projectives de Jacobi (U1 : V1 : W1) et d'un deuxième point P2 défini

par des deuxièmes coordonnées projectives de Jacobi ($U2 : V2 : W2$), les coordonnées du premier point P1 et celles du deuxième point P2 étant mémorisées dans des premiers et deuxièmes registres de la mémoire (4, 6, 8),
 5 le premier point et le deuxième point appartenant à la courbe elliptique,

les moyens de calcul programmés calculent des troisièmes coordonnées projectives de Jacobi ($U3 : V3 : W3$) définissant un troisième point P3,
 10 résultat de l'addition, par les relations suivantes :

$$\begin{aligned}
 U3 &= 2.b.U1^2.U2^2 \\
 &\quad + (aU1.U2 + W1.W2).(U1.W2+W1.U2) + 2V1.V2 \\
 V3 &= (U1^2.V2+U2^2.V1) * \\
 &\quad (4b.(U1.W2+U2.W1).W1.W2 \\
 15 &\quad - 8b^2.(U1.U2)^2 \\
 &\quad + a.[(2W1.W2)^2 - (aU1.U2+W1.W2)^2] \\
 &\quad + (W1^2.V2+W2^2.V1) * \\
 &\quad [(aU1.U2+W1.W2)^2 - (2aU1.U2)^2 + 4bU1.U2.(W1.U2+U1.W2)] \\
 &\quad - 4bU1.U2.(U1.W1.V2+U2.W2.V1)(aU1.U2-W1.W2) \\
 20 &\quad W3 = (aU1.U2-W1.W2)^2 - 4bU1.U2(U1.W2+U2.W1)
 \end{aligned}$$

puis mémorisent les troisièmes coordonnées projectives ($U3, V3, W3$) dans des troisièmes registres de la mémoire (6, 8).

25 5. Procédé selon la revendication 1, dans lequel la courbe elliptique est une courbe comprenant un seul point d'ordre deux et est définie par une équation quartique de type :

$$V^2 = \varepsilon.U^4 - 2\delta.U^2.W^2 + W^4,$$

30 ($U : V : W$) étant des coordonnées projectives de Jacobi d'un point P de la courbe elliptique, et ε, δ étant des paramètres de la courbe elliptique, le point de coordonnées ($0 : 1 : 1$) étant le point neutre O de la courbe elliptique, le point de coordonnées ($-U : +V : W$)
 35 étant le point inverse ($-P$) du point P($U : V : W$).

6. Procédé selon la revendication 5, dans lequel, pour réaliser l'addition du premier point P1 défini par des premières coordonnées projectives de Jacobi (U1 : V1 : W1) et du deuxième point P2 défini par des
 5 deuxièmes coordonnées projectives de Jacobi (U2 : V2 : W2), les coordonnées du premier point P1 et celles du deuxième point P2 étant mémorisées dans des premiers et deuxièmes registres de la mémoire (4, 6, 8), le premier point et le deuxième point appartenant à la
 10 courbe elliptique,

les moyens de calcul programmés calculent des troisièmes coordonnées projectives de Jacobi (U3 : V3 : W3) définissant un troisième point P3, résultat de l'addition, par les relations suivantes :

$$\begin{aligned}
 15 \quad U3 &= U1.W1.V2 + V1.U2.W2 \\
 V3 &= [(W1.W2)^2 + \varepsilon(U1.U2)^2] \\
 &\quad * [V1.V2 - 2\delta U1.U2.W1.W2] + 2\varepsilon.U1.U2.W1.W2 (U1^2 W2^2 + W1^2 U2^2) \\
 W3 &= (W1.W2)^2 - \varepsilon(U1.U2)^2
 \end{aligned}$$

puis mémorisent les troisièmes coordonnées
 20 projectives (U3, V3, W3) dans les troisièmes registres de la mémoire (6, 8).

7. Procédé selon l'une des revendications 5 à 6, dans lequel la courbe elliptique est définie en
 25 coordonnées affines par une équation du type :

$$Y^2 = \varepsilon.X^4 - 2\delta.X^2 + 1$$

(X, Y) étant des coordonnées affines d'un point P de la courbe elliptique.

8. Procédé selon la revendication 7, dans lequel, pour réaliser l'addition du premier point P1 défini par des premières coordonnées affines (X1, Y1) et du deuxième point P2 défini par des deuxièmes coordonnées affines (X2, Y2), les coordonnées du premier point P1 et celles
 35 du deuxième point P2 étant mémorisées dans des premiers et deuxièmes registres de la mémoire (4, 6, 8), le

premier point P1 et le deuxième point P2 appartenant à la courbe elliptique,

les moyens de calcul programmés calculent des troisièmes coordonnées affines (X3, Y3) définissant un
5 troisième point P3, résultat de l'addition, par les relations suivantes :

$$X3 = (X1.Y2 + Y1.X2) / [1 - \varepsilon(X1.X2)^2]$$

$$Y3 = \{ [1+\varepsilon(X1.X2)^2] \cdot [Y1.Y2 - 2\delta.X1.X2] + 2\varepsilon.X1.X2 \cdot (X1^2+X2^2) \} / [1 - \varepsilon(X1.X2)^2]$$

10 puis mémorisent les troisièmes coordonnées affines (X3, Y3) dans les troisièmes registres de la mémoire (6, 8).

9. Procédé selon l'une des revendications 5 à 8,
15 dans lequel la courbe elliptique est une courbe comprenant trois points d'ordre deux et a pour paramètre $\varepsilon = 1$.

10. Utilisation d'un procédé de calcul selon l'une
20 des revendications 1 à 9 dans un procédé de calcul de multiplication scalaire appliqué à des points d'une courbe elliptique.

11. Utilisation d'un procédé de calcul selon l'une
25 des revendications 1 à 9 dans un procédé cryptographique.

12. Composant électronique comprenant des moyens de calcul programmés pour mettre en œuvre un procédé selon l'une des revendications 1 à 9, les moyens de calcul
30 comprenant notamment une unité centrale (2) associée à une mémoire (4, 6, 8).

13. Composant électronique comprenant des moyens de mise en œuvre d'un algorithme cryptographique utilisant
35 un procédé selon l'une des revendications 1 à 9.

14. Carte à puce comprenant un composant électronique selon la revendication 12 ou 13.

1/1

