Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2542200 C 2009/02/24

(11)(21) **2 542 200**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(86) Date de dépôt PCT/PCT Filing Date: 2004/10/12
(87) Date publication PCT/PCT Publication Date: 2005/04/28
(45) Date de délivrance/Issue Date: 2009/02/24
(85) Entrée phase nationale/National Entry: 2006/04/10
(86) N° demande PCT/PCT Application No.: FR 2004/002579
(87) N° publication PCT/PCT Publication No.: 2005/038692
(30) Priorité/Priority: 2003/10/17 (FR0312152)

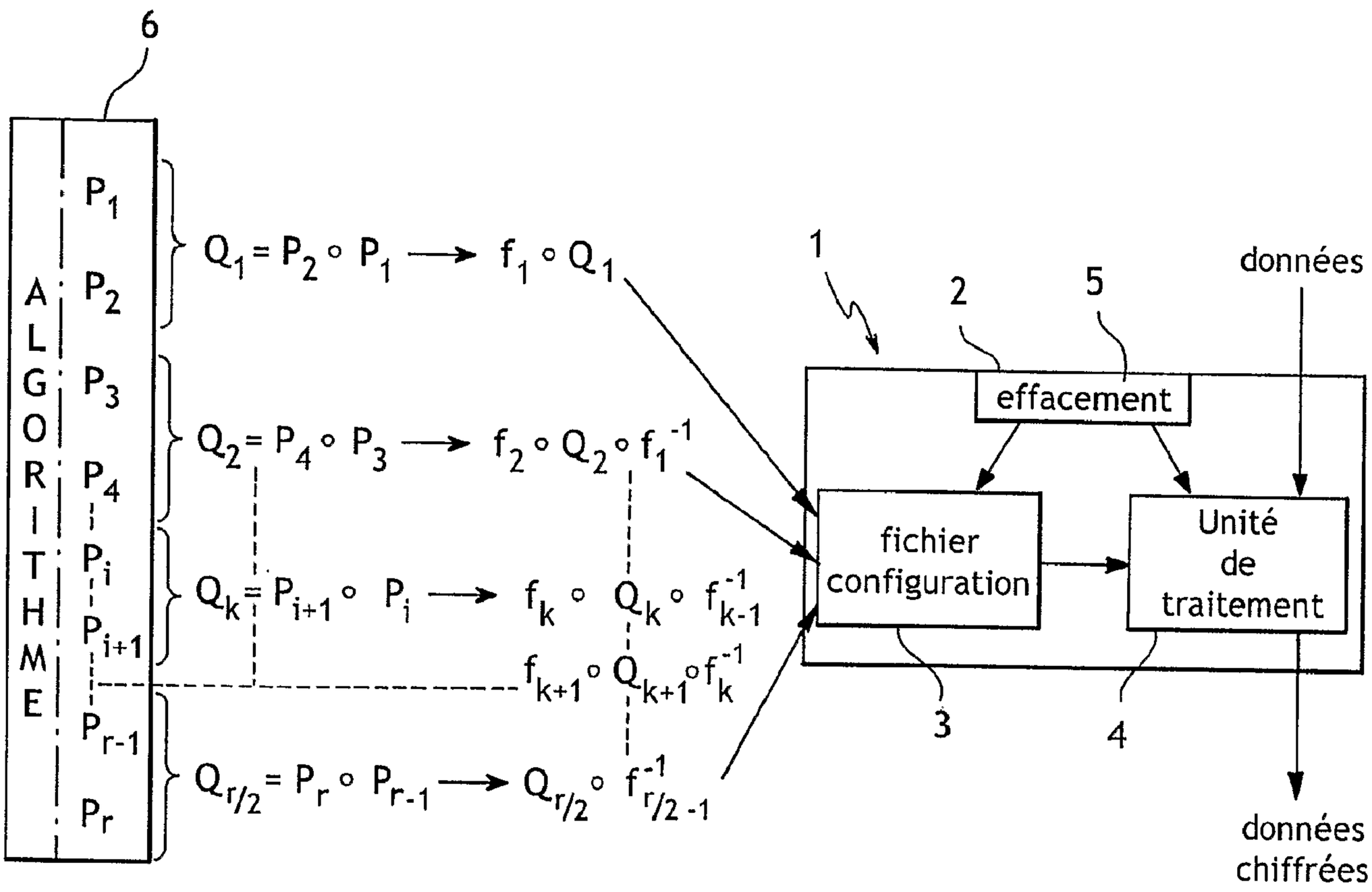
(51) Cl.Int./Int.Cl. *G06F 21/00* (2006.01)

(72) Inventeurs/Inventors:
CARLIER, VINCENT, FR;
CHABANNE, HERVE, FR;
DOTTAX, EMMANUELLE, FR

(73) Propriétaire/Owner:
SAGEM DEFENSE SECURITE, FR

(74) Agent: GOUDREAU GAGE DUBUC

(54) Titre : PROCEDE DE PROTECTION D'UN ALGORITHME CRYPTOGRAPHIQUE
(54) Title: METHOD FOR PROTECTION OF A CRYPTOGRAPHIC ALGORITHM



(57) Abrégé/Abstract:
Le procédé de protection d'un algorithme décomposable sous forme de polynômes initiaux (P_i) à au moins deux variables et ayant un degré au moins égal à deux, comporte les étapes de réaliser des polynômes combinés (Q_k) chacun obtenu à partir d'au moins deux polynômes initiaux (P_i, P_i+_1), et de mémoriser les polynômes combinés (Q_k) sous forme d'un fichier de configuration dans une mémoire (3) associée à une unité de traitement (4).

(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
28 avril 2005 (28.04.2005)

PCT

(10) Numéro de publication internationale
WO 2005/038692 A2

(51) Classification internationale des brevets[7] : G06F 21/00

(21) Numéro de la demande internationale :
PCT/FR2004/002579

(22) Date de dépôt international :
12 octobre 2004 (12.10.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0312152 17 octobre 2003 (17.10.2003) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **SAGEM SA** [FR/FR]; Le Ponant de Paris, 27 rue Leblanc, F-75015 PARIS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **CARLIER, Vincent** [FR/FR]; 15 rue Buffon, F-91400 ORSAY (FR). **CHABANNE, Hervé** [FR/FR]; 48 rue de la Marne, F-78200 MANTES LA JOLIE (FR). **DOTTAX, Emmanuelle** [FR/FR]; 29 rue de la Fontaine au Roi, F-75011 PARIS (FR).

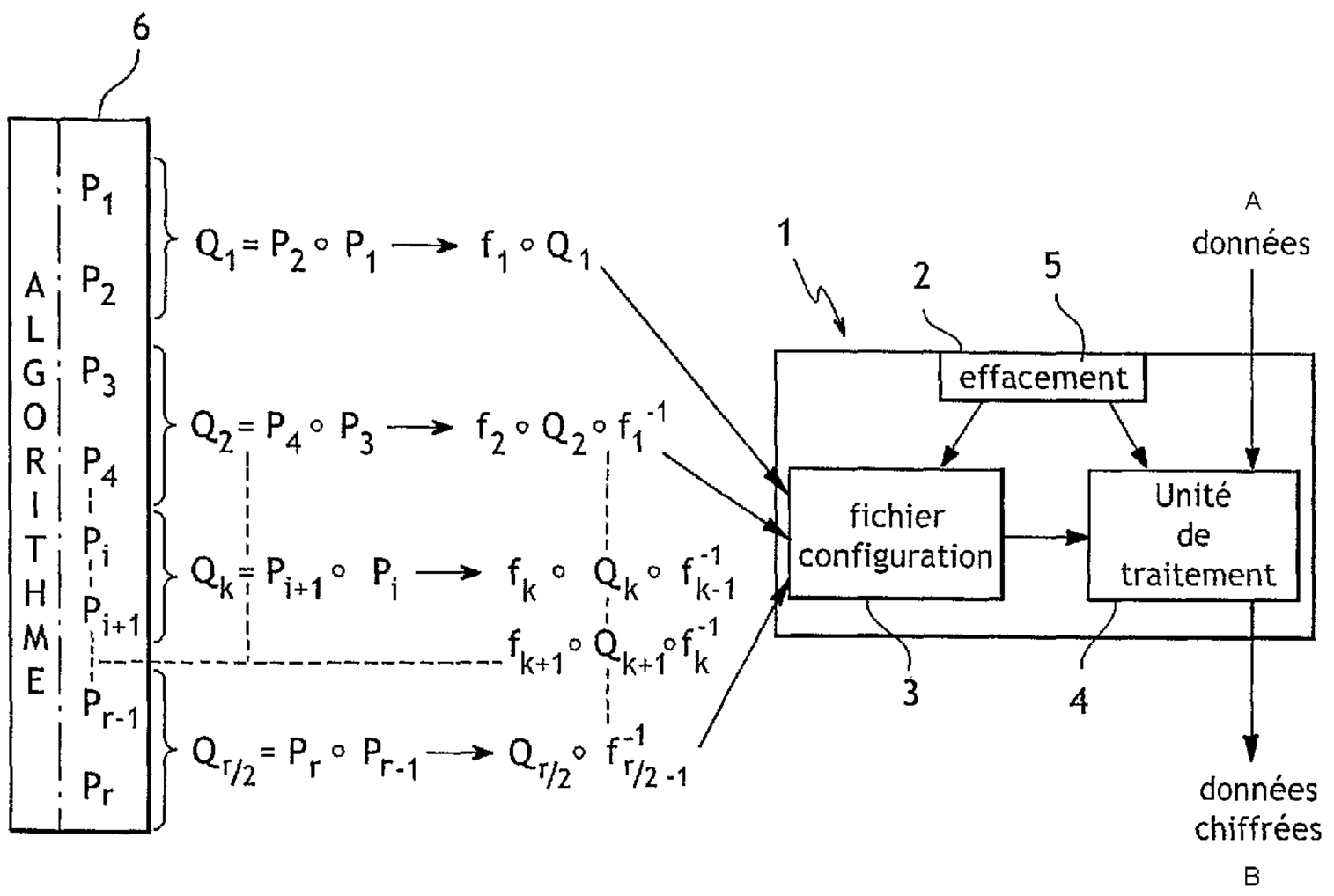
(74) Mandataires : **FRUCHARD, Guy** etc.; c/o CABINET BOETTCHER, 22 rue du Général Foy, F-75008 PARIS (FR).

(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, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,

[Suite sur la page suivante]

(54) Title: METHOD FOR PROTECTION OF A CRYPTOGRAPHIC ALGORITHM

(54) Titre : PROCEDE DE PROTECTION D'UN ALGORITHME CRYPTOGRAPHIQUE



6 ALGORITHM
3 CONFIGURATION FILE
4 PROCESSING UNIT
2 ERASURE
A DATA
B CIPHERED DATA

(57) **Abstract:** The invention relates to a method for protection of a decomposable algorithm in the form of initial polynomials (P_i) with at least two variables and having a degree of at least two, comprises the steps of generation of combined polynomials (Q_k), each obtained from at least two initial polynomials (P_i, P_i+_1) and memorising the combined polynomials (Q_k) in the form of a configuration file in a memory (3), associated with a processing unit (4).

[Suite sur la page suivante]

WO 2005/038692 A2

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 *(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, IT, 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).

Déclarations en vertu de la règle 4.17 :

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour la désignation suivante US*

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) Abrégé : Le procédé de protection d'un algorithme décomposable sous forme de polynômes initiaux (P_i) à au moins deux variables et ayant un degré au moins égal à deux, comporte les étapes de réaliser des polynômes combinés (Q_k) chacun obtenu à partir d'au moins deux polynômes initiaux (P_i, P_i+_1), et de mémoriser les polynômes combinés (Q_k) sous forme d'un fichier de configuration dans une mémoire (3) associée à une unité de traitement (4).

Procédé de protection d'un algorithme cryptographique.

La présente invention concerne un procédé de protection d'un algorithme cryptographique.

ARRIERE PLAN DE L'INVENTION

On sait que la façon la plus efficace de conserver la confidentialité lors d'une transmission de données est de chiffrer les données au moyen d'un algorithme cryptographique.

A cet effet on connaît des dispositifs comportant une unité de traitement programmable associés à un fichier de configuration comportant un algorithme cryptographique personnalisé. L'entité réalisant l'algorithme cryptographique personnalisé est généralement différente de l'entité réalisant le dispositif utilisant l'algorithme cryptographique. Afin de protéger l'algorithme cryptographique pendant le transport depuis son lieu d'élaboration jusqu'à son chargement dans le dispositif auquel il est destiné, on procède habituellement à un chiffrement de l'algorithme lui-même en utilisant une clé de protection. Sous cette forme chiffrée, l'algorithme cryptographique ne peut être exécuté par le dispositif auquel il est destiné. Lors du chargement de l'algorithme cryptographique dans le dispositif auquel il est destiné, un déchiffrement est donc effectué dans l'unité de traitement en utilisant la clé de protection qui y a été communiquée par le fabricant du dispositif et introduite par celui-ci dans l'unité de traitement. Le fabricant du dispositif ayant accès à la clé de protection, il est possible pour un fraudeur qui réussirait à obtenir d'une part l'algorithme cryptographique chiffré et d'autre part la clé détenue par le fabricant du dispositif, d'effectuer un déchiffrement de l'algorithme cryptographique lui permettant de reconstituer cet algorithme. En outre, après son déchiffrement l'algorithme n'est plus protégé de sorte qu'il est absolument nécessaire de disposer de moyens de sécurité particuliers pour protéger l'unité de

traitement pendant l'exécution de l'algorithme.

OBJET DE L'INVENTION

Un but de l'invention est de proposer un procédé de protection d'un algorithme cryptographique y compris lors de son exécution dans une unité de traitement sans qu'il soit nécessaire de faire intervenir le fabricant de l'unité de traitement.

BREVE DESCRIPTION DE L'INVENTION

En vue de la réalisation de ce but, on propose, selon l'invention, un procédé de protection d'un algorithme cryptographique décomposable sous forme de polynômes initiaux à au moins deux variables et ayant un degré au moins égal à deux, le procédé comportant les étapes de réaliser des polynômes combinés, chacun obtenu à partir d'au moins deux polynômes initiaux, et de mettre en œuvre les polynômes combinés dans l'unité de traitement.

Ainsi, la combinaison d'au moins deux polynômes initiaux ayant un degré au moins égal à deux, réalise un polynôme ayant un degré au moins égal à quatre dont il est extrêmement difficile de retrouver les constituants en particulier lorsque le nombre de variables de ces polynômes est suffisamment important. L'algorithme ainsi transformé est donc protégé et peut donc être transmis avec un degré de sécurité satisfaisant. Par ailleurs, les polynômes combinés sont directement exécutables au même titre que les polynômes initiaux. Aucune transformation n'est nécessaire lors de la configuration de l'unité de traitement de sorte que l'algorithme reste protégé pendant son exécution.

Selon une version avantageuse de l'invention, un effacement partiel de l'unité de traitement, et de la mémoire contenant le fichier de configuration lorsque la configuration est présente, est provoqué dans le cas d'une intrusion dans le dispositif. Dès l'instant où quelques informations sont manquantes la difficulté de

reconstitution de l'algorithme est considérablement augmentée de sorte qu'un effacement partiel seulement suffit à protéger l'algorithme.

Selon un autre aspect avantageux de l'invention, le procédé comporte en outre l'étape de combiner chaque polynôme combiné avec une fonction, et de combiner le polynôme combiné suivant avec une fonction inverse. Cette transformation complémentaire augmente encore la difficulté de retrouver les polynômes initiaux sans toutefois nuire au caractère exécutable du polynôme combiné en raison de l'élimination d'une fonction directe par la fonction inverse correspondante lors du passage d'un polynôme combiné au polynôme combiné suivant.

De préférence, la fonction combinée à chaque polynôme combiné est une fonction linéaire. Le degré du polynôme combiné reste alors inchangé, de sorte que l'espace pris en mémoire par le polynôme combiné reste lui-même inchangé.

DESCRIPTION DETAILLEE DE L'INVENTION

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de mise en œuvre particulier non limitatif de l'invention en relation avec la figure unique ci-jointe qui est un diagramme schématique illustrant le procédé selon l'invention.

En référence à la figure, le procédé de protection d'un algorithme cryptographique selon l'invention est destiné à être mis en œuvre dans un dispositif de chiffrement 1 comportant de façon connue en soi un boîtier 2 dans lequel est disposée une mémoire volatile 3 destinée à contenir un fichier de configuration et reliée à une unité de traitement 4 configurable par le fichier de configuration pour effectuer un chiffrement de données introduites dans le dispositif.

Egalement de façon connue en soi, le dispositif 1

comporte un organe d'effacement 5 relié à la mémoire 3 et à l'unité de traitement 4, pour assurer en cas d'intrusion un effacement au moins partiel des informations qu'elles contiennent. A cet effet la mémoire et l'unité de traitement 4 sont de préférence volatiles de sorte qu'une interruption même brève de l'alimentation provoque un effacement partiel des informations contenues dans la mémoire et/ou l'unité de traitement.

Selon l'invention, l'algorithme cryptographique 6 qui est destiné à être introduit dans le fichier de configuration 3 est tout d'abord divisé selon un procédé connu en soi, selon des rondes représentées par des polynômes initiaux P_1, P_2, P_3, P_4..., P_i, P_{i+1}..., P_{r-1}, P_r, à plusieurs variables et ayant un degré au moins égal à deux. Les polynômes initiaux sont déterminés en utilisant différentes clés (sauf répétition au hasard), ou différentes sous-clés d'une même clé. Les clés ou les sous-clés peuvent être totalement intégrées aux polynômes ou constituer des variables supplémentaires au sein des polynômes. Les polynômes initiaux P_i sont ensuite combinés, deux par deux dans le mode de mise en œuvre illustré, selon une combinaison mathématique de fonctions, pour obtenir des polynômes combinés $Q_1 = P_2 \circ P_1$, $Q_2 = P_4 \circ P_3$... $Q_k = P_{i+1} \circ P_i$..., $Q_{r/2} = P_r \circ P_{r-1}$. Lorsque les polynômes P_i ont un degré égal à deux, les polynômes combinés Q_k ainsi obtenus ont un degré égal à quatre.

Dans le mode de mise en œuvre préféré illustré, chaque polynôme Q_k est en outre combiné avec une fonction f_k, de préférence une fonction linéaire, et le polynôme combiné suivant est combiné de façon correspondante avec la fonction inverse f_k^{-1}, à l'exception bien entendu du premier et du dernier polynômes combinés qui ne sont combinés qu'avec une fonction directe pour l'un et une fonction inverse pour l'autre.

Avant son chargement dans la mémoire 3 sous forme

d'un fichier de configuration, l'algorithme cryptographique est donc représenté par les fonctions polynomiales $f_1 \circ Q_1$, $f_2 \circ Q_2 \circ f_1^{-1}$..., $f_k \circ Q_k \circ f_{k-1}^{-1}$, $f_{k+1} \circ Q_{k+1} \circ f_k^{-1}$,..., $Q_{r/2} \circ f_{r/2-1}^{-1}$.

Bien entendu, l'invention n'est pas limitée au mode de mise en œuvre décrit et on peut y apporter des variantes de réalisation sans sortir du cadre de l'invention tel que défini par les revendications.

En particulier, bien que les rondes initiales aient été représentées sous forme d'un seul polynôme initial par ronde, chaque ronde peut contenir plusieurs polynômes initiaux. Les polynômes initiaux peuvent donc être combinés au sein d'une même ronde ou en combinant plusieurs rondes entre elles.

Bien que le procédé ait été décrit en relation avec un dispositif comprenant une unité de traitement 4 associée à une mémoire 3 destinée à recevoir l'algorithme sous forme d'un fichier de configuration, ce qui permet d'effectuer une modification de la configuration sans avoir à effectuer un retour du dispositif en atelier, on peut prévoir une mise en œuvre directe de l'algorithme dans l'unité de traitement par une configuration de l'unité de traitement en atelier. Dans ce cas la configuration ne peut plus être modifiée sans un retour en atelier.

Bien que le procédé selon l'invention ait été décrit en combinant les polynômes initiaux deux à deux, il peut être nécessaire pour certains algorithmes de regrouper les polynômes élémentaires selon un nombre supérieur à deux. Par exemple pour l'algorithme dénommé DES dans lequel les rondes sont entrelacées, il est nécessaire de combiner plus de deux polynômes initiaux pour obtenir des polynômes combinés exécutables de façon sûre selon le procédé décrit ci-dessus.

Bien que l'invention ait été décrite avec une

étape comprenant une combinaison avec une fonction et la fonction inverse, on peut prévoir de constituer le fichier de configuration simplement à partir des polynômes combinés Q_k.

Au lieu d'effectuer la combinaison des différents polynômes combinés Q_k avec des fonctions f_k différentes pour chacun des polynômes combinés Q_k comme décrit ci-dessus, on peut combiner chaque polynôme combiné avec la même fonction f puis avec la fonction inverse f^{-1}.

REVENDICATIONS

1. Procédé de protection d'un algorithme cryptographique (6) en vue de son exécution dans un dispositif (1) comprenant une unité de traitement programmable (4), l'algorithme étant décomposable sous forme de polynômes initiaux (P_i) à au moins deux variables et ayant un degré au moins égal à deux, caractérisé en ce que le procédé comporte les étapes de réaliser des polynômes combinés (Q_k) chacun obtenu à partir d'au moins deux polynômes initiaux (P_i, P_{i+1}), et de mettre en œuvre les polynômes combinés (Q_k) dans l'unité de traitement programmable (4).

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre l'étape de mémoriser les polynômes combinés (Q_k) sous forme d'un fichier de configuration chargé dans une mémoire (3) associée à l'unité de traitement (4).

3. Procédé selon la revendication 2, caractérisé en ce que la mémoire (3) et l'unité de traitement programmable (4) sont associés à un organe d'effacement (5) provoquant, dans le cas d'une intrusion dans le dispositif, un effacement de l'unité de traitement (4), et un effacement de la mémoire (3) contenant le fichier de configuration lorsque la configuration est présente dans cette mémoire.

4. Procédé selon la revendication 1, caractérisé en ce qu'il comporte l'étape de combiner chaque polynôme combiné (Q_k) avec une fonction (f_k), et de combiner le polynôme combiné suivant (Q_{k+1})avec une fonction inverse (f_k^{-1}).

5. Procédé selon la revendication 4, caractérisé en ce que la fonction (f_k) combinée à chaque polynôme combiné (Q_k) est une fonction linéaire.

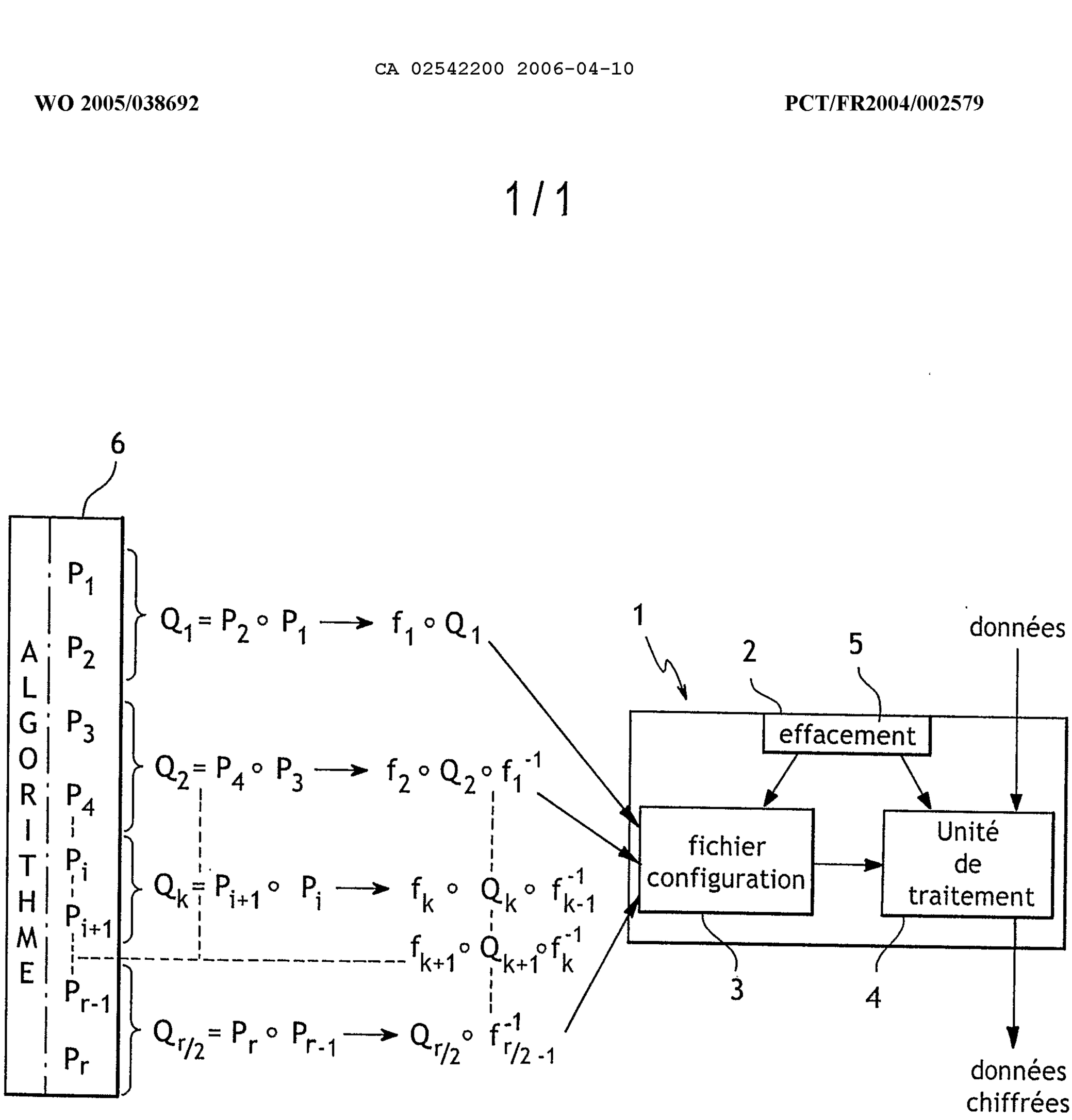
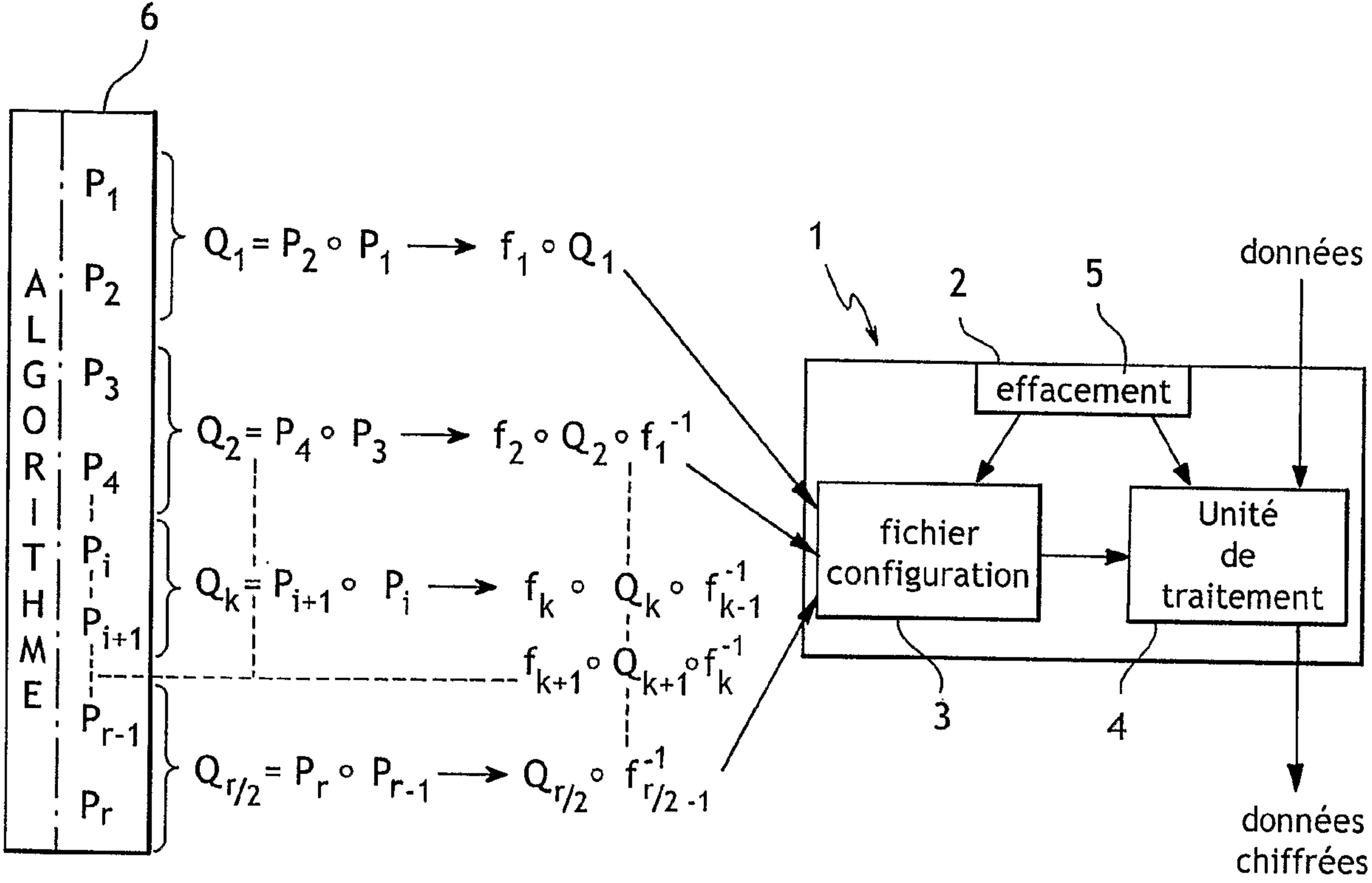

6
ALGORITHME
P1
P2
P3
P4
Pi
Pi+1
Pr-1
Pr
Q1 = P2 ∘ P1 → f1 ∘ Q1
Q2 = P4 ∘ P3 → f2 ∘ Q2 ∘ f1-1
Qk = Pi+1 ∘ Pi → fk ∘ Qk ∘ fk-1-1
fk+1 ∘ Qk+1 ∘ fk-1
Qr/2 = Pr ∘ Pr-1 → Qr/2 ∘ fr/2 -1-1
1
2
5
effacement
fichier configuration
Unité de traitement
3
4
données
données chiffrées

FIG.1


6
A L G O R I T H M E
P1
P2
P3
P4
Pi
Pi+1
Pr-1
Pr
Q1 = P2 ∘ P1 → f1 ∘ Q1
Q2 = P4 ∘ P3 → f2 ∘ Q2 ∘ f1-1
Qk = Pi+1 ∘ Pi → fk ∘ Qk ∘ fk-1-1
fk+1 ∘ Qk+1 ∘ fk-1
Qr/2 = Pr ∘ Pr-1 → Qr/2 ∘ fr/2 -1-1
1
2
5
données
effacement
fichier configuration
Unité de traitement
3
4
données chiffrées