

(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
17 juin 2010 (17.06.2010)

PCT

(10) Numéro de publication internationale
WO 2010/066478 A1

(51) Classification internationale des brevets :
G06F 21/24 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2009/061069

(22) Date de dépôt international :
27 août 2009 (27.08.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
08305934.5 12 décembre 2008 (12.12.2008) EP

(71) Déposant (pour tous les États désignés sauf US) :
GEMALTO SA [FR/FR]; 6 rue de la Verrerie, F-92190 Meudon (FR).

(72) Inventeur; et

(75) Inventeur/Déposant (pour US seulement) :
GONZALVO, Benoît [FR/FR]; 27 Quartier des Charrons, F-13420 Gemenos (FR).

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Suite sur la page suivante]

(54) Title : METHOD FOR SECURING THE FRAGMENTED USE OF A DIGITAL DATUM

(54) Titre : PROCÉDÉ DE SÉCURISATION DE L'UTILISATION PARCELLAIRE D'UNE DONNÉE NUMÉRIQUE

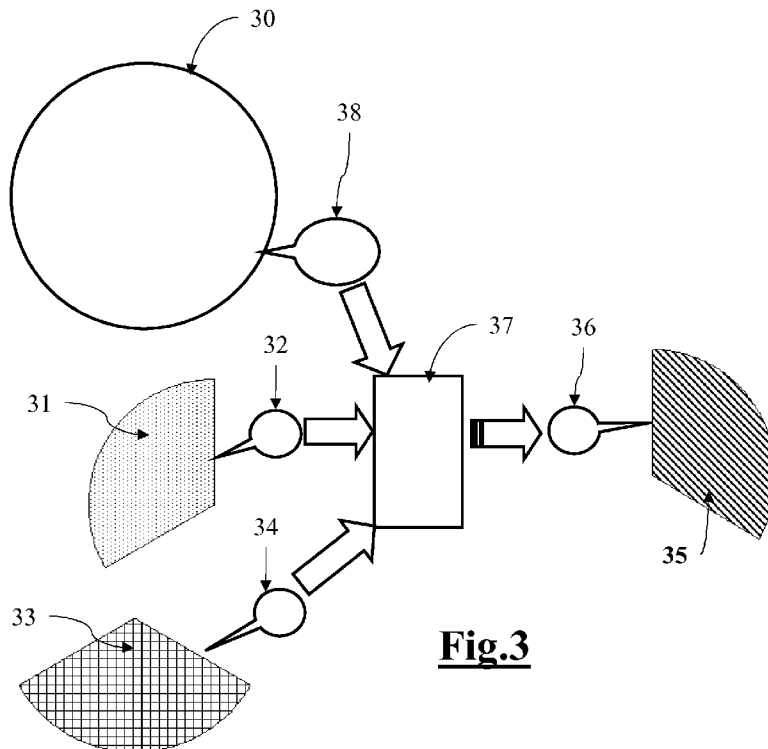


Fig.3

(57) Abstract : The invention relates to a method for securing the fragmented use of a sensitive datum without preliminarily storing the securing values for each potential fragment. The values are calculated on the fly without relying on the fragments to which they are connected so as to prevent any potential corruption of the data before associating the securing value thereto.

(57) Abrégé : Procédé de sécurisation de l'utilisation parcellaire d'une donnée sensible sans stockage préalable de valeurs de sécurisation pour chacune des parcelles potentielles. Ces valeurs sont calculées à la volée, sans s'appuyer sur les parcelles auxquelles elles sont liées afin de se prémunir contre une éventuelle altération des données avant l'association de la valeur de sécurisation.

WO 2010/066478 A1



Publiée :

— avec rapport de recherche internationale (Art. 21(3))

**- Procédé de sécurisation de l'utilisation parcellaire d'une donnée
numérique -**

La présente invention concerne la sécurité des données numériques, en particulier les données pouvant être lues ou utilisées dans un appareil numérique portable et, en particulier, concerne un procédé pour
5 sécuriser l'utilisation parcellaire d'une donnée numérique protégée face aux attaques par faute, lors de son exploitation par un appareil numérique portable.

Un appareil portable désignera par la suite tout appareil numérique portable tel qu'un ordinateur
10 portable mais aussi tout appareil doté d'un microcontrôleur réunissant un processeur et des mémoires, tel qu'une carte à puce.

Les données électroniques prennent chaque jour un
15 rôle plus important dans la vie de tout un chacun, notamment grâce à la vulgarisation des appareils électroniques portatifs grand public tels que les appareils photographiques numériques, les dispositifs multimédia tels que les lecteurs mp3, les « GPS » qui
20 contiennent vos destinations ou encore les téléphones portables qui embarquent de plus en plus de fonctionnalités telles que la gestion des agendas, la gestion des carnets d'adresse. Si ces données augmentent en nombre, leurs natures restent
25 généralement limitées, et il est aisé de les regrouper,

par exemple en fonction de leur type : Image, Vidéo, carte de visite, texte ...

L'interconnexion grandissante des systèmes électroniques, et notamment la circulation des données, rendent celle-ci de plus en plus sujettes à des attaques.

Ces attaques sont communément divisées en trois grandes familles :

- 10 Les attaques d'intégrité,
- Les attaques de confidentialité
- Les attaques de déni de service.

Les attaques d'intégrité visent à altérer le contenu d'une donnée, généralement à l'insu de son destinataire légitime. Ce genre d'attaque est typiquement mené afin de modifier des informations dans une donnée. Par exemple, lors d'un échange entre un terminal bancaire et le serveur de la banque, un attaquant peut avoir un fort intérêt à modifier le montant de la transaction. Dans un tout autre domaine, lors d'une authentification avec une carte d'identité électronique, l'attaquant peut avoir un intérêt à modifier certains champs, par exemple le nom dans le cas d'une carte d'identité volée.

Ces attaques sont généralement menées en interceptant l'échange de données entre l'émetteur légitime, et le destinataire légitime. Une fois le message intercepté, il est interprété afin d'en comprendre le contenu. Il est ensuite modifié, et enfin renvoyé au destinataire

légitime, qui le recevra pensant qu'il vient de l'expéditeur légitime.

Cette attaque s'appuie sur un mécanisme appelé en anglais « man in the middle » qui permet à l'attaquant
5 d'intercepter et de réémettre un message entre deux acteurs sans que ceux-ci ne s'aperçoivent de sa présence, l'attaquant se faisant passer pour un récepteur légitime, face à l'émetteur, et comme un émetteur légitime face au récepteur.

10

Les attaques de confidentialité sont menées afin de recueillir de l'information. Le but de l'attaquant est de lire le maximum de données échangées entre l'émetteur légitime, et le destinataire légitime. Selon
15 les objectifs de l'attaque, celle-ci peut se mener avec un "man in the middle", comme dans la description de l'attaque précédente, ou bien sans.

Dans le cas où un « man in the middle » est mis en place, une fois le message intercepté, il est
20 interprété afin d'en comprendre le contenu. Il est ensuite renvoyé au destinataire légitime, qui le recevra pensant qu'il vient de l'expéditeur légitime. Dans ce mode d'implémentation d'une attaque en confidentialité les acteurs légitimes de l'échange de
25 données ne sont pas informés de la fuite d'information.

Dans le cas où un "man in the middle" n'est pas réalisé entre l'émetteur et le récepteur, l'attaquant va intercepter tout ou partie des informations échangées, et va en prendre connaissance. Cette attaque va
30 rapidement être détectée car les informations interceptées sont perdues. Ainsi le récepteur ne reçoit pas les informations qui lui sont destinées. Le plus souvent c'est l'émetteur qui va détecter l'attaque car

il n'aura pas, de la part du récepteur, la réaction qu'il attendait suite à son envoi d'informations.

Ces attaques sont généralement menées afin de découvrir des informations secrètes comme par exemple des codes secrets.

Les attaques en dénie de service sont un peu marginales au regard des deux précédentes, car leur but est d'interrompre le fonctionnement du système. En effet si les attaques ont toutes un objectif plus ou moins délictuel, un moyen simple de nuire aux acteurs d'un système est d'interrompre son fonctionnement. Ce genre d'attaque peut se faire par exemple en empêchant deux acteurs de communiquer, ce qui rend leur synergie nulle.

Une autre méthode peut consister en l'émission d'une grande quantité d'information à destination de tout ou partie des acteurs du système attaqué. Cette technique, aussi appelée « bombing » en anglais permet de surcharger les dispositifs électroniques partis du système, et par la même de les empêcher de dédier du temps et de la puissance de calcul pour faire les actions qui sont attendues d'eux. Une autre méthode plus complexe peut consister en la mise en place d'un « man in the middle » entre deux acteurs, et en l'altération de tout ou partie des informations échangées. Dans ce mode d'attaque, les messages seront bien envoyés et reçus, mais leur contenu sera tout ou partiellement incompréhensible, et donc inexploitable. Ce genre d'attaque plus difficile à mettre en œuvre a généralement pour objectif de ralentir sa détection.

Ainsi, une vérification de l'intégrité des données est importante dans la gestion normale des données, mais

elle crucial en particulier face aux attaques dites attaques par faute.

Les attaques par faute sont basées sur une altération du traitement normal d'une information afin de
5 provoquer un état « anormal ». Dans certains cas cet état « anormal » va permettre à l'attaquant d'obtenir de l'information indument, ou bien va faire en sorte par exemple que le processus électronique ne réalise pas certaines étapes de sécurité, ou d'altérer une
10 lecture ou une écriture en mémoire. Des fautes particulièrement élaborées peuvent permettre de modifier la valeur d'une donnée en mémoire, voire même pendant son traitement.

Cette altération du traitement normal peut se faire de
15 deux manières, soit par une perturbation physique, soit par une perturbation logique.

Dans le cas d'une perturbation physique, c'est une variation de l'environnement du dispositif électronique, pendant sont fonctionnement, qui produit
20 la perturbation. Par exemple un choc thermique ou une source lumineuse particulièrement intense peut provoquer une telle perturbation.

Dans le cas d'une perturbation logique, l'attaquant soumet au programme des données que celui-ci ne
25 s'attend pas à obtenir, et espère donc provoquer une perturbation. Cela peut se faire par l'utilisation de données « trop » grandes, ou par exemple qui ne serait de la nature attendues.

Toutes ces attaques peuvent être limitées en
30 garantissant, avant toute utilisation l'intégrité des données. Le terme de donnée désigne ici tout élément numérique pouvant entrer dans l'exécution d'un programme informatique. Le mot donnée désigne notamment

les variables, les operateurs, les adresses mémoire, les éventuels registres et leurs pointeurs et tout autre élément de programmation.

- 5 Afin de se prémunir d'éventuelles attaques, les solutions existantes tendent à affecter, à chaque donnée, une donnée de contrôle. Une vérification de la relation entre une donnée et sa donnée de contrôle permet de vérifier que celle-ci n'a pas subi d'attaque
10 d'intégrité.

Ces solutions présentent un problème majeur : une multiplication des données engendre une multiplication des données de contrôle, et vue la quantité de données croissante, ces données de contrôle prennent une place
15 qui devient problématique dans l'univers des dispositifs électroniques mobiles, par exemple tels que les téléphones portables ou les carte a puce.

La présente invention propose de rassembler des données
20 dans des supra-données, elles protégées par l'usage de données de contrôle, et lors de l'utilisation d'une parcelle de ces supra-données, de générer une valeur de contrôle associée à cette parcelle.

25 Plus précisément l'invention est dans un premier temps un procédé de sécurisation de l'utilisation parcellaire d'une donnée sensible dite supra-donnée, ce procédé comprend une étape d'application d'un mode sécurisé dans lequel, dans une étape préalable une
30 première fonction d'extraction est appliquée à ladite supra-donnée afin d'obtenir une valeur de contrôle liée

la supra-donnée par l'intermédiaire d'une fonction prédéterminée,

Lors de chaque utilisation parcellaire de la supra-donnée, le procédé comprend notamment les étapes
5 de :

- lecture d'une parcelle de la supra-donnée dite « parcelle lue »,
- extraction, au cours de laquelle une seconde fonction d'extraction est appliquée à chacune des
10 autres parcelles composant la supra-donnée afin d'obtenir, pour chacune d'elle, une valeur de contrôle dite résiduelle,
- déduction de la valeur de contrôle, dite valeur de référence, de la parcelle lue par
15 l'application d'une fonction mathématique prenant entre autre comme paramètres la valeur de contrôle de la supra-donnée et les valeurs de contrôle résiduelles.

Le procédé peut comprendre en outre une étape
20 consistant à

- vérifier que ladite valeur de référence et ladite parcelle lue, sont liées par la fonction prédéterminée.

25 La supra-donnée peut être composée d'au moins deux parcelles distinctes. Dans un mode particulier d'implémentation, ces parcelles ne sont pas de même nature. Dans un mode particulier d'implémentation, ces parcelles ne sont pas de même taille.

La fonction prédéterminée utilisée par le procédé peut définir un morphisme de groupe.

Dans un mode d'implémentation, le mode d'exécution sécurisé peut être appliqué continuellement.

5 Dans un mode d'implémentation, le mode d'exécution sécurisé peut être appliqué de façon aléatoire.

Dans un mode d'implémentation, le mode d'exécution sécurisé peut être appliqué sur détection d'une condition particulière, par exemple en fonction de
10 l'interprétation d'une partie du code.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description faite à titre d'exemple non limitatif et en regard des
15 dessins annexés parmi lesquels :

- la figure 1 illustre une supra-donnée
- la figure 2 illustre l'extraction d'une parcelle d'une supra-donnée
- la figure 3 illustre la génération d'une donnée
20 de contrôle d'une parcelle.

Comme illustré dans la figure 1, l'invention propose donc de sécuriser l'utilisation parcellaire d'une donnée 10 appelée supra-donnée, elle même
25 protégée par une valeur de contrôle 14 appelée valeur de contrôle globale. Cette supra-donnée est elle même composée de parcelles 11, 12, 13. Dans un mode préféré d'implémentation, les parcelles ne sont pas de taille identique. De même, les parcelles ne sont pas
30 obligatoirement de même nature. Ici le terme de nature s'entend au sens de type de donnée, ainsi une parcelle

peut être par exemple constituée de données, une autre contenir du texte exécutable, et une troisième un mélange des deux. L'utilisation des données s'entend d'un point de vue informatique, par des opérations
5 telles que par exemple la lecture ou la modification. L'utilisation d'une valeur de contrôle permet, à tout moment de vérifier que la donnée que l'on manipule n'a pas été altérée de manière frauduleuse. Cette vérification peut se faire en calculant une valeur de
10 contrôle candidate grâce à l'application d'une fonction d'extraction sur la donnée, et en comparant cette valeur de contrôle candidate avec la valeur de contrôle initialement associée à la donnée.

15 Afin de pouvoir faire cette vérification à tout moment dans le programme informatique qui manipule la donnée ainsi protégée, il convient que toute modification licite de cette donnée entraîne un recalcul de la valeur de contrôle afin que ces deux
20 entités numériques soient toujours reliées par la fonction qui les associe.

Pour ce faire, les données et les valeurs de contrôle correspondantes sont donc liées entre elles
25 par l'intermédiaire d'une fonction de contrôle prédéterminée, dotée de propriétés mathématiques particulières comme expliquées ci-après.

Ainsi, soit V l'espace de valeurs sur des registres de longueur s . Pour des registres de longueur
30 32 bits, on a :

$$V = [-2147483648, 2147483647] = [-2^{31}, 2^{31}-1]$$

Soit O l'ensemble V , avec les opérations logiques et arithmétiques classiques suivantes $(+, -, *, /, \&, |)$.

Soit F l'ensemble V avec l'ensemble d'opérations symbolisées de la manière suivantes $(\star, \boxtimes, \odot, \blacklozenge, \square, \circ)$.

5 La fonction de contrôle Chk selon l'invention peut alors être décrite de la manière suivante:

$Chk : O \longrightarrow F$, de telle sorte que pour toute opération op dans l'ensemble $(+, -, *, /, \&, |)$, il existe une opération correspondante cop dans l'ensemble

10 $(\star, \boxtimes, \odot, \blacklozenge, \square, \circ)$ telle que:

$$Chk(a \ op \ b) = Chk(a) \ cop \ Chk(b)$$

Par exemple, la fonction $\sim$ précédemment décrite du complément à 1 peut être écrite comme un cas particulier de la fonction Chk de la façon suivante :

$$15 \quad \sim : (V, (+, -, *, /, \&, |)) \longrightarrow (V, (\star, \boxtimes, \odot, \blacklozenge, \square, \circ))$$

$$a \quad | \longrightarrow \sim a$$

avec

$$\sim(a + b) = \sim a \star \sim b = \sim a + \sim b + 1$$

$$\sim(a - b) = \sim a \boxtimes \sim b = \sim a - \sim b - 1$$

20

Mathématiquement, la fonction de contrôle Chk peut être définie comme un morphisme de groupe de l'espace O vers l'espace F , respectant l'ensemble des opérations dans F .

25 Ainsi, on peut voir que pour toute opération logique ou arithmétique agissant sur une ou des données dans l'espace V , qui est l'espace arithmétique classique des ordinateurs, il est possible de trouver un calcul équivalent en utilisant la fonction Chk telle

30 que définie, utilisant un opérateur cop lié à

l'opérateur op mis en œuvre dans le premier calcul par l'intermédiaire de la fonction Chk, et agissant sur une ou des données dites de contrôle, liées aux données utilisées dans le premier calcul par l'intermédiaire de la fonction Chk.

La fonction de contrôle selon l'invention à la particularité de permettre, connaissant la valeur de contrôle d'une supra-donnée composée de N parcelles, et les valeurs de contrôle de N-1 parcelles, il est possible de générer la valeur de contrôle de la N^{ième} parcelle.

Dans un mode d'implémentation de l'invention, cette fonction peut avoir deux forme, une forme appelée CHK qui permet d'associer une valeur de contrôle appelée « CHK(a) » à une donnée « a », et une forme appelée GCHK pour « Global CHK » qui permet d'associer une valeur de contrôle à la supra-donnée en fonction des valeur de contrôle des différentes parcelles qui la composent.

Un exemple de fonction peut être obtenu par la fonction identité :

CHK : $a \mapsto \text{CHK}(a) = a$

La valeur de contrôle associée à une donnée est alors définie comme une simple redondance de cette donnée.

Un deuxième exemple est obtenu en utilisant la fonction ~ décrite précédemment.

Un troisième exemple peut être obtenu en utilisant des fonctions mathématiques généralement utilisées dans les applications cryptographiques :

CHK : $a \mapsto g^a$ avec g le générateur d'un groupe cyclique.

On voit alors que $\text{CHK}(a + b) = g^{(a+b)} = g^a \cdot g^b = \text{CHK}(a) \cdot \text{CHK}(b)$ est bien un morphisme de groupe.

Dans la figure 2, une parcelle 22 de la supra-donnée 20 est extraite, par exemple afin d'être lue. La supra-donnée est protégée par sa valeur de control 24, mais la parcelle 22 doit obtenir une valeur de control 25 afin de pouvoir être utilisée en toute sécurité.

Si une fonction d'extraction est appliquée à la parcelle 22 afin de lui générer une valeur de contrôle 25, alors il est possible à un agent malicieux d'altérer la valeur de la parcelle 22, avant que la valeur de contrôle 25 ne soit affectée, par exemple grâce à une attaque par faute. Dans ce cas, la parcelle 22 deviendrait une parcelle corrompue 26, à laquelle serait associé une valeur de contrôle 27. Hors cette valeur de contrôle 27 et la parcelle 26 seraient effectivement liés par la fonction prédéfinie. Et il serait dès lors impossible de mettre en évidence la falsification qui a été opérée sur la parcelle 22.

La mise en œuvre de l'invention permet d'associer une valeur de contrôle à une parcelle, sans s'appuyer sur celle-ci. Ce qui empêche une éventuelle action frauduleuse, de perturber cette affectation de valeur de contrôle.

La figure 3 illustre un mode préféré de mise en œuvre de l'invention dans lequel la parcelle 35 est extraite de la supra-sonnée 30, par exemple pour être lue.

Des lors que le contrôleur de la mémoire qui contient
5 la supra-donnée 30 reçoit cette requête, la valeur de contrôle 387 associée à la supra-donnée 30 est lue, et les autres parcelles entrant dans la composition de la supra-donnée 30 sont également lues. Dans notre exemple se sont les parcelles 31 et 33. Dans l'exemple de la
10 figure 3, une fonction d'extraction est appliquée à chacune des parcelles 31 et 33 afin d'extraire leurs valeur de control respectives 32 et 34. Une fonction 37 est appliquée aux valeurs de contrôle 38, 32, et 34 afin d'obtenir la valeur de contrôle 36, associée à la
15 parcelle 35.

La fonction 37 est très fortement liée à la fonction GCHK qui a permit de construire la valeur de control globale de la supra-donnée, à partir des valeurs de contrôle des différentes parcelles qui la composent.
20 Ainsi, si la fonction GCHK utilisée est l'addition, alors la fonction 37 qui permet de retrouver la valeur de control d'une parcelle de la supra-donnée a partir des valeurs de contrôle des autres parcelles est la soustraction.

25 En effet, si la fonction CHK est la fonction identité, et la fonction GCHK est l'addition, alors un exemple d'implémentation peut être:

- $CHK(a) = a,$
- $CHK(a + b + c) = GCHK.$

- Alors on peut retrouver le checksum de « a » en recalculant le checksum de « b » et « c » mais sans utiliser « a » en calculant :

Valeur de contrôle de "a" = $GCHK - CHK(b) - CHK(c)$

5

Un autre exemple d'implémentation s'appuyant sur la fonction identité et la fonction « ou exclusif » (aussi appelé XOR)

- $CHK(a) = a$
- 10 • $GCHK(a, b, c) = a \text{ XOR } b \text{ XOR } c,$
- Alors Valeur de contrôle de "a" = $a = GCHK(a, b, c) \text{ XOR } b \text{ XOR } c$

15 Dans un exemple d'implémentation s'appuyant sur la fonction cryptographique g déjà définie, alors on peut utiliser la fonction « * ». Ainsi :

- $CHK(a) = g^a$
- $GCHK(a, b, c) = g^{(a+b+c)} = g^a * g^b * g^c = CHK(a) * CHK(b) * CHK(c)$
- 20 • Ainsi Valeur de contrôle de "a" = $GCHK(a, b, c) / (CHK(b) * CHK(c))$

25 Ainsi, une valeur de control a été associée à une parcelle de donnée sans avoir eut besoin d'utiliser cette parcelle.

L'invention permet donc de limiter les risques

L'invention permet donc de ne stocker que très peu de
30 valeurs de contrôle en regroupant un maximum de donnée

dans des supra-données, de plus l'invention permet de n'affecter des valeurs de contrôle qu'aux parcelles réellement utilisées.

REVENDICATIONS

1. Procédé de sécurisation de l'utilisation
parcellaire d'une donnée sensible dite supra-donnée,
caractérisé en ce que il comprend une étape
5 d'application d'un mode sécurisé dans lequel, dans une
étape préalable une première fonction d'extraction est
appliquée à ladite supra-donnée afin d'obtenir une
valeur de contrôle liée à ladite supra-donnée par
l'intermédiaire d'une fonction prédéterminée,

10 Lors de chaque utilisation parcellaire de ladite
supra-donnée, le procédé comprend notamment les étapes
de :

- lecture d'une parcelle de ladite supra-donnée
dite « parcelle lue »,
- 15 - extraction, au cours de laquelle une seconde
fonction d'extraction est appliquée à chacune des
autres parcelles composant ladite donnée sensible afin
d'obtenir, pour chacune d'elle, une valeur de contrôle
dite résiduelle,
- 20 - déduction de la valeur de contrôle, dite
valeur de référence, de la parcelle lue par
l'application d'une fonction mathématique prenant entre
autre comme paramètres la valeur de contrôle de la
supra-donnée et les valeurs de contrôle résiduelles.

25

2. Procédé selon la revendication 1, caractérisé
en ce qu'il comprend en outre une étape consistant à

- vérifier que ladite valeur de référence et ladite parcelle lue, sont liées par ladite fonction prédéterminée.

3. Procédé selon la revendication 1, caractérisé en ce que ladite supra-donnée est composée d'au moins deux parcelles distinctes.

4. Procédé selon la revendication 3, caractérisé en ce que lesdites parcelles ne sont pas de même nature.

5. Procédé selon la revendication 3, caractérisé en ce que lesdites parcelles ne sont pas de même taille.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la fonction prédéterminée utilisée définit un morphisme de groupe.

7. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que le mode d'exécution sécurisé est appliqué continuellement.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le mode d'exécution sécurisé est appliqué de façon aléatoire.

9. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le mode

d'exécution sécurisé est appliqué sur détection d'une condition particulière.

10. Procédé selon la revendication 9, caractérisé
5 en ce que la condition d'application du mode d'exécution sécurisé est fonction de l'interprétation d'une partie du code.

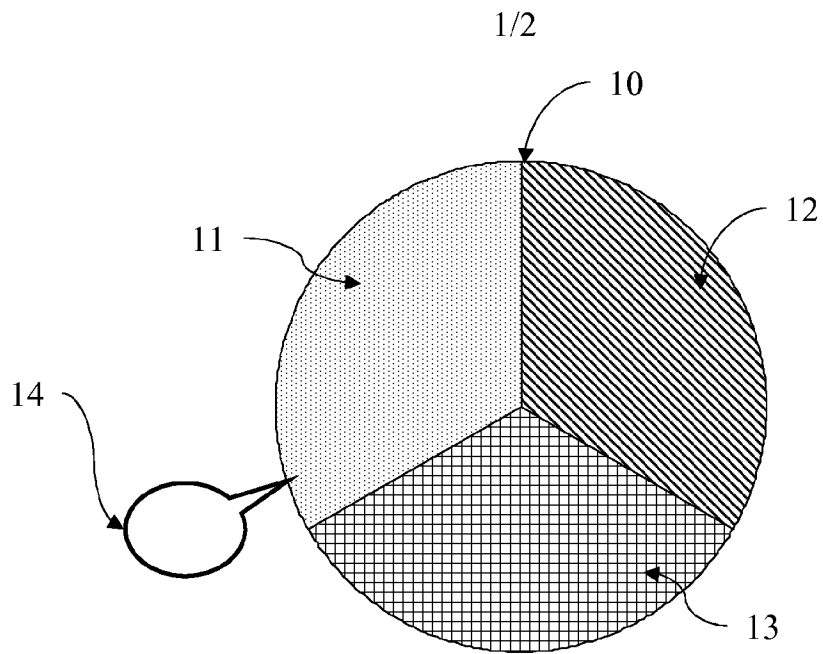


Fig.1

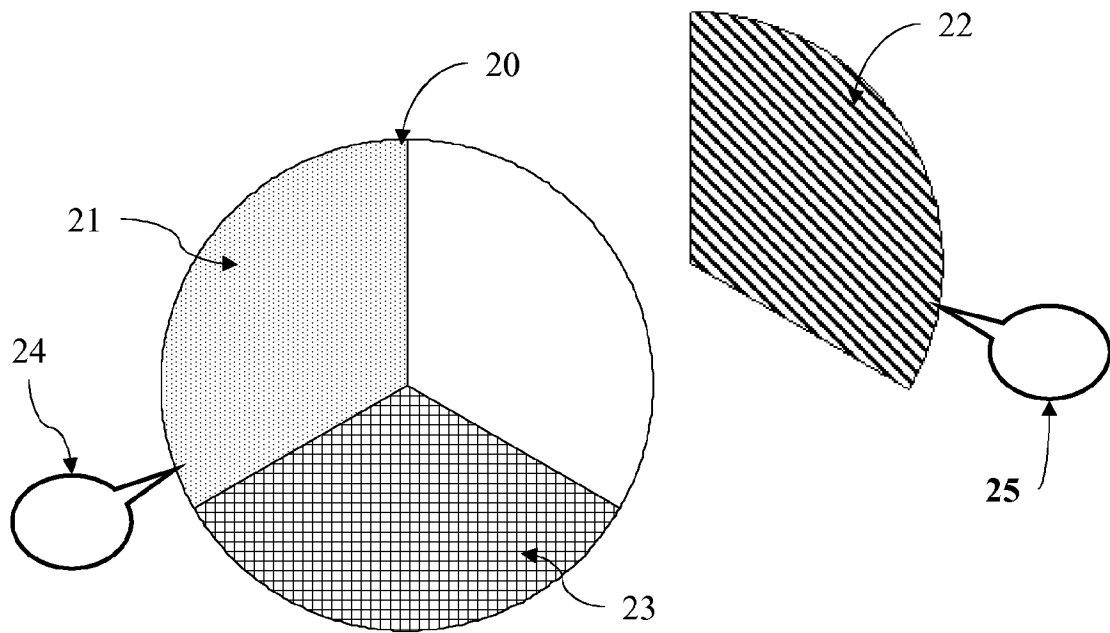
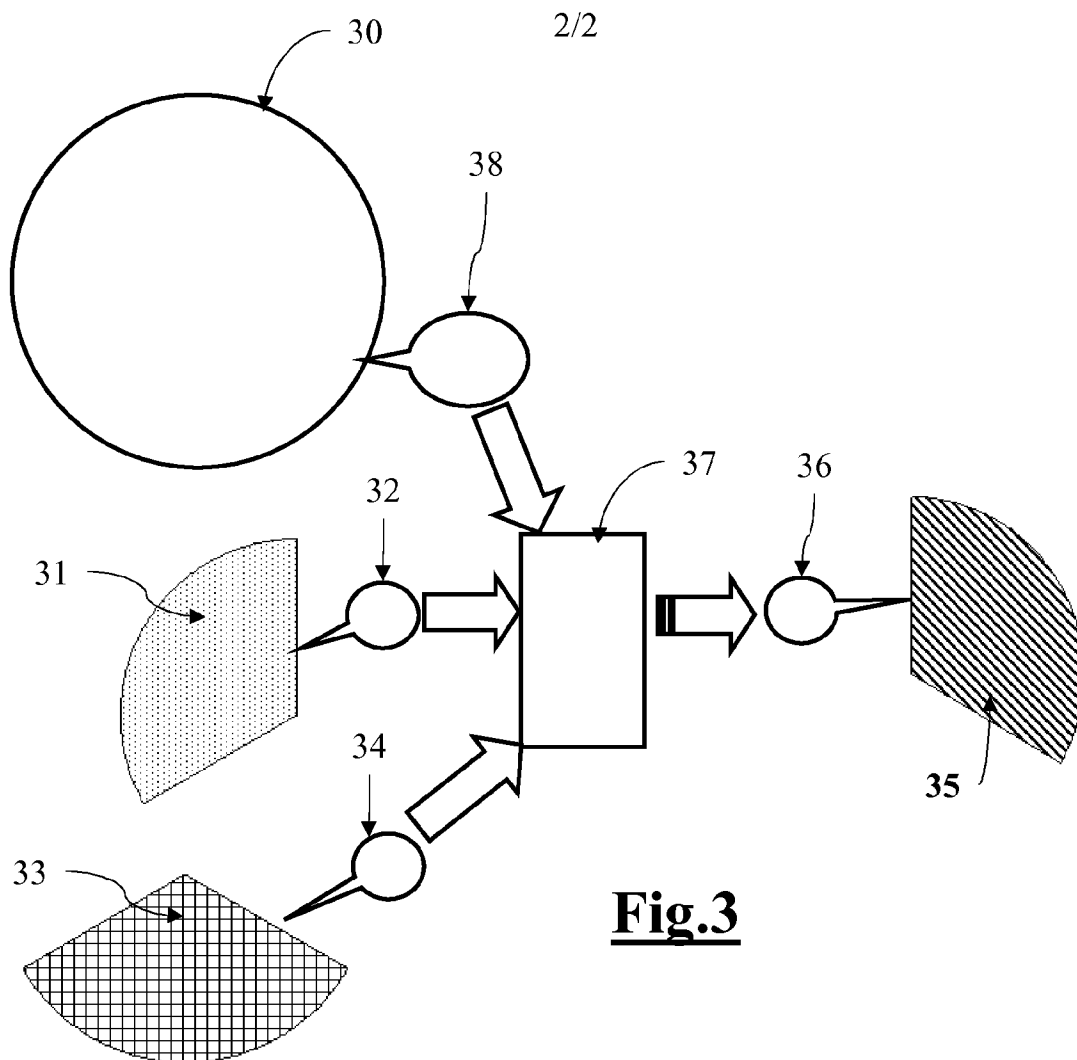


Fig.2



INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/061069

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/24

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)

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 881 404 A (GEMPLUS CARD INT [FR]) 23 January 2008 (2008-01-23) paragraphs [0019] - [0024] paragraphs [0032] - [0054] paragraphs [0064] - [0075] -----	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

9 décembre 2009

Date of mailing of the international search report

16/12/2009

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Alecu, Mihail

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/061069

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
EP 1881404	A	23-01-2008	EP	2047366 A1	15-04-2009
			WO	2008009697 A1	24-01-2008

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2009/061069

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06F21/24		
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) 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 cela est réalisable, termes de recherche utilisés) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	EP 1 881 404 A (GEMPLUS CARD INT [FR]) 23 janvier 2008 (2008-01-23) alinéas [0019] - [0024] alinéas [0032] - [0054] alinéas [0064] - [0075] -----	1-10
☐ 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'appartenant 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'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément "Y" document particulièrement pertinent; l'invention 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 9 décembre 2009		Date d'expédition du présent rapport de recherche internationale 16/12/2009
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Alecu, Mihail

Renseignements relatifs aux membres de familles de brevets

PCT/EP2009/061069

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)