(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 juin 2012 (28.06.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/085215 A1

(51) Classification internationale des brevets :
H04L 9/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2011/073810

(22) Date de dépôt international :
22 décembre 2011 (22.12.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1005116 23 décembre 2010 (23.12.2010) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **THALES** [FR/FR]; 45 rue de Villiers, F-92200 Neuilly Sur Seine (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **MARCELLO, Sandra** [FR/FR]; 160 Boulevard de Valmy, BP 82, F-92704 Colombes Cedex (FR). **CAPMAN, François** [FR/FR]; 160 Boulevard de Valmy, BP 82, F-92704 Colombes Cedex (FR). **DELORME-GUILLON, Gaëtan** [FR/FR]; 160 Boulevard de Valmy, BP 82, F-92704 Colombes Cedex (FR). **SALIBA, Eric** [FR/FR]; 160 Boulevard de Valmy, BP 82, F-92704 Colombes Cedex (FR).

(74) Mandataires : **DUDOUIT, Isabelle** et al.; Immeuble Visium, 22 Avenue Aristide Briand, F-94117 Arcueil (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, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,

[Suite sur la page suivante]

(54) Title : METHOD AND SYSTEM FOR MULTI-THRESHOLD MULTIMODAL AUTHENTICATION USING SECRET SHARING

(54) Titre : PROCEDE ET SYSTEME POUR L'AUTHENTIFICATION MULTI-MODALE MULTI-SEUIL UTILISANT LE PARTAGE DE SECRET

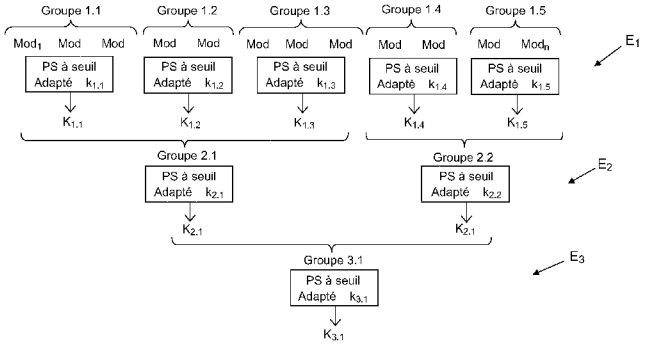


FIG.1

Groupe = Group
PS à seuil adapté = Adapted threshold secret sharing
Mod = Mod

(57) Abstract : The invention relates to a method and a system for authenticating one or more users or objects, one or more users together with one or more objects, using a multimodal authentication principle with Modi modalities and multiple thresholds. To begin, n Modi modalities (i = 1 à n) are assigned to different groups Gi,j. Each group Gi,j is used to perform a multimodal authentication with threshold ki,j with a secret sharing scheme: the first subscript (i) is the subscript of the stage in the "cascade", and the second subscript (j) is the subscript of the group considered in the stage. For all notations comprising two subscripts, the first refers to the current stage of the cascade and the second is a number that can be used to differentiate the different data on a given stage. For each of the groups Gi,j, a cryptographic key Ki'j is created if the group authentication threshold ki,,j is reached. Subsequently, new groups Gi+1,j are formed with keys Ki,j for a given stage i and multimodal authentication is performed, and so on.

(57) Abrégé :

[Suite sur la page suivante]

WO 2012/085215 A1

LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

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

L'invention concerne un procédé et un système pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets en utilisant un principe d'authentification multimodale avec les modalités Modi et multi seuils. Au départ, n modalités Modi (i = 1 à n) sont réparties en différents groupes Gi,,j. Chaque groupe Gi,,j est utilisé pour faire une authentification multimodale à seuil ki, j avec un schéma de partage de secret : le premier indice (i) est l'indice de l'étage de la « cascade », et le deuxième indice (j) est l'indice du groupe considéré dans la l'étage. Pour toutes les notations comportant deux indices, le premier se réfère donc à l'étage de la cascade sur lequel on se trouve et le deuxième est un numéro qui permet de distinguer les différentes données sur un étage donné. Pour chacun des groupes Gi,,j, une clé cryptographique Ki'j est créée si le seuil d'authentification du groupe ki,,j est atteint. On forme ensuite avec ces clés Ki,J pour un étage i donné de nouveaux groupes Gi+1,,j où l'on procède aussi à une authentification multimodale et ainsi de suite.

PROCEDE ET SYSTEME POUR L'AUTHENTIFICATION MULTI-MODALE MULTI-SEUIL UTILISANT LE PARTAGE DE SECRET

L'objet de la présente invention concerne un procédé et un système permettant une authentification multimodale, multi-seuil, utilisant un schéma de partage de secret (PS). Le procédé s'applique pour authentifier un individu, un système ou un objet grâce à cette authentification multimodale, multi-seuil.

Elle est notamment utilisée pour générer une clé cryptographique dépendante de m modalités avec un ou plusieurs seuils d'authentification multimodale k.

Le mot « donnée biométrique », dans la suite de la description, couvre les empreintes digitales, l'iris, ...etc. toutes les données biométriques connues aujourd'hui ou dans les années à venir.

L'invention est notamment utilisée pour l'authentification :

- d'un ou plusieurs supports en utilisant des PUFs,
- d'une ou plusieurs personnes grâce à la biométrie multimodale,
- avec une modalité principale et des modalités secondaires,
- dans le domaine de la téléphonie, la radio, les aéroports, de manière plus générale tous les systèmes d'authentification biométriques ou dans les systèmes nécessitant une authentification grâce aux PUFs

Le problème de l'authentification d'un individu, d'un objet ou d'un système se rapporte souvent à l'extraction d'une donnée connue à partir d'une donnée floutée et la génération de données d'authentification ou de clés cryptographiques. Les fonctions associées sont généralement : l'identification et l'authentification et, la génération de clés cryptographiques.

Un secure sketch est défini plus précisément dans l'article principal connu dans ce domaine publié par Dodis et al., intitulé « Fuzzy

extractors : How to generate strong keys from biometrics and other noisy data » Eucrocypt 2004, LCNS, vol 3027, pp 523-540 qui traite du problème du caractère non uniforme des données mesurées et de la présence de bruit. Pour rendre les données stables malgré la présence de bruit, les auteurs de cet article proposent l'utilisation d'un extracteur flou. Une possibilité pour construire un extracteur flou est l'utilisation de deux primitives. Un premier module, désigné par l'expression anglo-saxonne « secure sketch » permet la conciliation de l'information, c'est-à-dire le rétablissement d'une valeur systématiquement identique en sortie pour une même donnée d'entrée, et un second module permet de rendre uniforme la sortie de l'extracteur flou par application d'une fonction d'extraction d'aléa sur ladite sortie, préalablement stabilisée. L'extracteur flou fonctionne en deux phases : l'enrôlement et la correction. La phase d'enrôlement peut n'être exécutée qu'une seule fois ; elle produit à partir d'une donnée de référence, notée w, issue d'une mesure d'une donnée confidentielle W fournie en entrée, une donnée publique, notée s et qualifiée dans la plupart du temps de « sketch ». Classiquement, la donnée de référence w peut être obtenue via une première mesure issue d'un traitement d'une donnée confidentielle W reçue par un capteur ou un composant électronique. A titre illustratif, la donnée confidentielle W est une empreinte digitale et la donnée de référence w est la donnée caractéristique obtenue par une première mesure de cette empreinte par un capteur. Seule la donnée publique s est enregistrée, la donnée de référence w étant confidentielle. La donnée publique joue donc un rôle dans la reconstruction de la mesure confidentielle de référence w à partir d'une donnée bruitée w '.

La demande de brevet WO 2008/010773 décrit un système de génération d'une clé biométrique à partir de données biométriques mettant en œuvre un schéma multimodal.

Le document de Changlu Lin et al, intitulé « Ideal PPerfect Multilevel Threshold Secret Sharing Scheme, divulgué lors de la

conférence Information assurance and Security en 2009, pages 118-121, XP031543915, décrit un schéma à seuil multi hiérarchique. Le secret est divisé en n shareholers de façon telle que toute personne autorisée puisse le reconstituer.

Le document de Tamir Tassa, intitulé « Hierarchical Threshold Secret Sharing » publié dans le journal of cryptography, pages 237-264, XP 019487898, février 2007 décrit lui aussi un schéma à seuil multi hiérarchique. La nouveauté du schéma proposé est l'usage de dérivées de polynôme de façon à générer des partages plus faibles pour les utilisateurs de niveaux inférieurs.

La demande de brevet WO 2007/0691146 concerne une méthode pour convertir un ensemble de données en un ensemble de bits chiffrés représentant l'ensemble des données.

L'idée mise en œuvre dans la présente invention est, notamment, de créer des groupes qui vont générer chacun une clé cryptographique si les groupes sont valides, c'est-à-dire que le nombre de modalités valides dans le groupe est supérieur à un seuil fixé. Il sera ensuite possible de recréer des groupes avec ces clés cryptographiques afin de les authentifier séparément, toujours avec la possibilité d'utiliser des seuils. Chaque groupe de clés cryptographiques crée une nouvelle clé cryptographique, et il est alors possible de créer de nouveaux groupes et ainsi de suite.

L'invention concerne un procédé pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets, en utilisant un principe d'authentification multimodale avec différentes modalités Modi (i=1 à n) réparties dans différents groupes Gi,j, un groupe étant utilisé pour faire de l'authentification multimodale à seuil d'authentification ki,j avec un schéma de partage de secret, i étant l'indice de l'étage Ei d'une cascade et j l'indice du groupe considéré dans un étage et des multi seuils dans un

système d'authentification comportant plusieurs étages de traitement caractérisé en ce qu'il comporte au moins les étapes suivantes :

au niveau du premier étage E1 du système :

a1) une première étape consiste à générer une clé cryptographique K en utilisant des mesures $w_1=w(mod_1)$, …, $w_n=w(mod_n)$ sur lesdites modalités Mod_1 ,… Mod_n,

soit L_m la liste des m modalités dont la clé cryptographique en sortie du système dépend, ces modalités et leur nombre sont choisis en fonction d'une application donnée,

soit une donnée $K=f(L_m)$ avec f une fonction dont les propriétés sont telles que la donnée K est non prédictible, le procédé exécute les étapes suivantes

a2) une deuxième étape d'enrôlement des secure sketches où l'on associe à chaque modalité Modi un secure sketch SSi,

a3) une troisième étape d'initialisation du partage de secret en distribuant le secret K entre les différentes modalités Modi, et en générant des données qui sont mémorisées dans une donnée publique D,

a4) une quatrième étape de stockage de données en déterminant les modalités valides en utilisant une fonction non inversible et en stockant en faisant varier l'indice de l'étage de i=1 à n les valeurs $v_i=h'(w(mod_i))$ obtenues en exécutant la fonction non inversible, où h' est une fonction de hachage,

a5) une cinquième étape de recherche de k modalités valides en corrigeant pour chacune des mesures des n modalités correspondant à $w'(mod_1),…,w'(mod_n)$, ces mesures avec les secure sketches associés SSi pour obtenir $w''(mod_1),…,w''(mod_n)$, données corrigées ou non en fonction de la validité de la modalité et qui vont être utilisées pour déterminer les modalités valides et pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets.

Selon une variante de mise en œuvre une liste L' de modalités valides est construite en exécutant les étapes suivantes :

Soit L' la liste des modalités valides, le procédé fait varier l'indice de l'étage i variant de1 à n

Si $h'(w''(mod_i))=v_i$, on ajoute i dans la liste de validité L',

Si $|L'|<k$, il existe moins de K éléments dans la liste, on fait plus varier l'indice de l'étage,

Sinon, on effectue le partage de secret avec k modalités appartenant à L' et on génère la clé associée à l'étage 1 et à un groupe composé de plusieurs modalités Modi.

Pour exécuter l'étape a4) les modalités sont déterminées, par exemple, en exécutant une fonction de hachage h' et en stockant pour i=1 à n les $v_i=h'(w(mod_i))$ obtenues grâce à l'exécution de la fonction de hachage.

Pour les étages de rang i supérieur à 1, disposés après le premier étage E1 de la cascade, le procédé utilise, par exemple, les valeurs des clés cryptographiques Ki-1,j pour le partage de secret.

Le procédé peut comporter au moins les étapes suivantes :

La génération de la clé cryptographique pour un groupe Gi

Soient $w_1=K_{i,1}$, …, $w_n=K_{i,n}$ les clés cryptographiques appartenant à un groupe de l'étage i,

Soit L_m la liste des clés $K_{i,j}$ dont on veut que la clé cryptographique en sortie $K_{i+1,1}$ du système dépende, soit alors la clé cryptographique $K_{i+1,1}=f(L_m)$,

L'initialisation du partage de secret en distribuant le secret $K_{i+1,1}$ entre les différentes clés $K_{i,j,}$

<u>Autres données à stocker</u>

Pour le partage de secret, on détermine quelles modalités sont valides afin d'en sélectionner k valides en choisissant une fonction de hachage h' ou une fonction non inversible et on stocke pour i=1 à n les $v_i=h'(w(mod_i))$,

Au cours de la phase d'utilisation :

La recherche de $k_{i+1,1}$ clés valides

Soit L' la liste des modalités valides.

Pour i=1 à n

Si $h'(w_i)=v_i$, ajouter i dans L',

Si $|L'|< k_{i+1,1}$, on s'arrête.

Sinon, effectuer le partage de secret avec $k_{i+1,1}$ modalités appartenant à L'.

Soient $k_{i+1,1}$ modalités au moins valides,

les données disponibles à ce stade sont les w_i valides ainsi que la donnée D qui permet d'effectuer le partage de secret et à partir desquelles on trouve alors la clé $K_{i+1,1}$.

Le schéma de partage de secret est, par exemple, le partage de secret de Shamir et le procédé comporte au moins les étapes suivantes :

c1) la génération de la clé cryptographique

Soient $w_1=w(mod_1)$, ..., $w_n=w(mod_n)$ des mesures sur les modalités Mod_1 ,... Mod_n, L_m la liste des m modalités dont la clé cryptographique en sortie du système dépend et $K=f(L_m)$ la clé cryptographique,

c2) on effectue les enrôlements des secure sketches avec les données w_1, ..., w_n pour obtenir les sketches $s_1=s(mod_1)$, ..., $s_n=s(mod_n)$.

c3) on initialise le partage de secret

Le secret est S = K que l'on doit partager entre n modalités avec un seuil k, pour cela on effectue les actions suivantes :

- Choisir une fonction de hachage h,
- Le secret est S=K avec un seuil du partage de secret soit k avec k variant de 2 à n-1,
- Choisir aléatoirement un polynôme $f(x)= S + a_1x + ... + a_{k-1}x^{k-1}$,
- Pour chaque modalité, c'est-à-dire pour i=1,...,n, associer le couple $(h(w_i), f(h(w_i)))$ où $w_i = w(mod_i)$,

On stocke ensuite dans la variable D (donnée publique) les données $f(h(w_i))$, ordonnées des points, pour i=1 à n,

On choisit une fonction de hachage h' et stocker pour i=1 à n les v_i=h'(w(mod_i)) qui permettront de déterminer les modalités valides dans le partage de secret, avec h' une fonction différente de h,

Au cours de la phase d'utilisation

c4) on recherche de k modalités valides

Pour chacune des mesures des n modalités w'(mod_1),…,w'(mod_n) on corrige ces données avec les secure sketches pour obtenir w''(mod_1),…,w''(mod_n),

Soit L' la liste des modalités valides.

Pour i=1 à n

Si h'(w''(mod_i))=v_i, ajouter i dans L'.

Si |L'|<k , arrêter,

Sinon, on effectue le partage de secret avec k modalités appartenant à L',

c5) le partage de secret

Les données disponibles à ce stade sont les w_i=w(mod_i) valides ainsi que D = {f(h(w_i))}.

Le recouvrement du secret s'effectue de la façon suivante :

- A partir de D, former les couples (h(w_1), f(h(w_1))), …., (h(w_k), f(h(w_k))),
- En utilisant l'interpolation (de Lagrange par exemple) avec ces couples, retrouver le polynôme f(x) et donc son ordonnée à l'origine S=K.

Pour l'étape de génération de la clé cryptographique, le procédé comporte, par exemple, au moins les étapes suivantes :

pour f concaténer les w_i pour i dans L_m rangés par ordre croissant puis hacher le tout avec une fonction de hachage h_1,

ou choisir une fonction de hache h_1, puis pout tout i dans L_m calculer $h_1(w_i)$, puis additionner les différents éléments de L_m avec l'opération $\oplus$.

La fonction de partage de secret utilisée est une fonction choisie parmi la liste suivante :

Le partage avec des Xor $\oplus$(Xor), le secret $s \in \{0;1\}^l$, on choisit aléatoirement $s_1,\ldots,s_{n-1}$ dans $\{0;1\}^l$ puis on calcule $s_n = s \oplus s_1 \oplus \ldots \oplus s_{n-1}$, et on distribue tous les s_i. On adapte ce schéma en prenant s=K puis, pour i=1 à n en posant s_i=w(mod$_i$) et $D = s \oplus s_1 \oplus \ldots \oplus s_n$;

Pour retrouver le secret, les n modalités doivent être valides et on retrouve le secret en calculant $s = D \oplus w_1 \oplus \ldots \oplus w_n$.

L'invention concerne aussi un système pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets en utilisant un principe d'authentification multimodale avec les modalités Modi et multi seuils caractérisé en ce qu'il comporte au moins les éléments suivants : plusieurs capteurs adaptés à mesurer des modalités associées à un ou plusieurs utilisateurs, une unité de calcul ou processeur permettant d'exécuter les étapes du procédé présentant une ou plusieurs des caractéristiques précitées, des modules de mémorisation des données telles que les secure sketches.

D'autres caractéristiques et avantages de la présente invention apparaîtront mieux à la lecture de la description qui suit donnée à titre illustratif et nullement limitatif annexé des figures qui représentent :

- La figure 1, un exemple d'architecture globale de la notion de cascade utilisée par le procédé selon l'invention,
- La figure 2, la phase d'enrôlement des secure sketches dans un groupe donné,
- La figure 3, la phase d'initialisation de partage de secret dans un groupe donné,
- La figure 4, la phase d'utilisation pour un groupe donné,
- La figure 5, un exemple de dispositif permettant la mise en œuvre du procédé selon l'invention.

La figure 1 schématise un exemple de mise en œuvre du procédé selon l'invention dans le cas d'une cascade comprenant trois étages de traitement, cet exemple étant donné à titre illustratif.

Notations utilisées dans la description de l'invention.

Au départ, n modalités Modi (i = 1 à n) sont réparties en différents groupes Gi,j. Chaque groupe Gi,j est utilisé pour faire une authentification multimodale à seuil ki ,j avec un schéma de partage de secret : le premier indice (i) est l'indice de l'étage de la « cascade », et le deuxième indice (j) est l'indice du groupe considéré dans la l'étage. Pour toutes les notations comportant deux indices, le premier se réfère donc à l'étage de la cascade sur lequel on se trouve et le deuxième est un numéro qui permet de distinguer les différentes données sur un étage donné.

Pour chacun des groupes Gi,j, une clé cryptographique Ki'j est créée si le seuil d'authentification du groupe ki,j est atteint. On forme ensuite avec ces clés Ki,j pour un étage i donné de nouveaux groupes Gi+1,j où l'on procède aussi à une authentification multimodale et ainsi de suite.

Au niveau du premier étage 1, E_1, de la cascade, le procédé traite des données floues Modi avec le système détaillé ci-après qui utilise des secure sketches (en abrégés SS) connus de l'Homme du métier et des schémas de partage de secret (PS) à seuil ki,j pour effectuer l'authentification multimodale à seuil du groupe. Le schéma de partage de secret nécessite une adaptation pouvoir être utilisé. A partir du deuxième étage E2, les données ne sont plus floues : c'est-à-dire que ces données sont soit valides, soit non valides, du fait du traitement au niveau du PS à seuil.

Authentification multimodale à seuil

Nous allons maintenant décrire les briques de partage de secret PS à seuil adapté, ki,j pour i = 1. Pour un étage de rang i>=2, il n'est pas nécessaire d'utiliser le même traitement car les données considérées ne

sont plus floues. Le traitement alors appliqué est le même mais en enlevant les secure sketches qui sont alors inutiles vu que les données ne sont pas floues.

Initialisation du procédé selon l'invention décrit pour chacune des briques

a1) Génération de la clé cryptographique

Une première étape consiste à générer une clé cryptographique.

Soient $w_1=w(mod_1)$, …, $w_n=w(mod_n)$ des mesures sur les modalités Mod_1 ,… Mod_n. Notons que les n modalités considérées ici appartiennent à un même groupe G1,j. Sachant cela, les indices correspondant à l'étage et au groupe considérés seront omis. En toute rigueur le nombre de modalités dépend également du groupe, ici dans un souci de simplification des notations, comme il n'y a pas d'ambiguïté il sera noté n.

Soit L_m la liste des m modalités dont la clé cryptographique en sortie du système va dépendre, ces modalités et leur nombre est choisi en fonction de l'application.

Soit alors la clé cryptographique $K=f(L_m)$; f est une fonction dont les propriétés sont telles que la clé K est non prédictible et possède toutes les propriétés d'une bonne clé cryptographique selon les critères de l'Homme de l'art. C'est une donnée secrète définie au moment de l'initialisation du système. En cas de nécessité due à l'application, cette donnée K peut ne pas être une clé cryptographique mais n'importe quelle autre donnée secrète : un mot de passe, une identité, …

Exemple : pour f(.), il est possible de concaténer les w_i pour i dans L_m rangés par ordre croissant puis de hacher le tout avec une fonction de hachage h_1.

Si $L_5=\{1, 2, 5, 7, 12\}$, $K = h_1(w_1|| w_2|| w_5|| w_7|| w_{12})$.

Autre exemple : il consiste à choisir une fonction de hachage h_1, puis pour tout i dans L_m, calculer $h_1(w_i)$. Ensuite, par exemple si $L_5=\{1, 2, 5, 7, 12\}$, on pose $K=f(L_m)=h_1(w_1) \oplus h_1(w_2) \oplus h_1(w_5) \oplus h_1(w_7) \oplus h_1(w_{12})$.

a2) Enrôlement des secure sketches selon un mode opératoire connu de l'Homme du métier et représenté à la figure 2

A chaque modalité Modi est associé un secure sketch SSi. Les enrôlements des secure sketches sont effectués avec les données w_1, ..., w_n pour obtenir les sketches $s_1=s(mod_1)$, ..., $s_n=s(mod_n)$ selon la représentation de la figure 2, et d'un principe connu de l'Homme du métier.

a3) Initialisation du partage de secret

Cette phase illustrée par exemple à la figure 3 a pour but de distribuer le secret K entre les différentes modalités Modi. Il n'est pas possible d'utiliser directement les schémas classiques de partage de secret car une partie des morceaux de secret distribués est imposé par les modalités : il faut adapter la partage de secret. L'exemple du partage de secret de Shamir adapté est détaillé dans la suite de la description.

Le partage de secret engendre des données qui doivent être stockées (ces données sont publiques) ; la donnée D contient ces éléments.

a4) Autres données à stocker

Pour le partage de secret, il est nécessaire de savoir quelles modalités sont valides afin d'en sélectionner k valides et de pouvoir ainsi reconstituer le secret. Pour cela, on choisit par exemple une fonction de hachage h' et on stocke pour i=1 à n les $v_i=h'(w(mod_i))$ obtenues grâce à l'exécution de la fonction de hachage.

Phase d'utilisation illustrée à la figure 4

a5)Recherche de k modalités valides

Pour chacune des mesures des n modalités correspondant à $w'(mod_1),\ldots,w'(mod_n)$, le procédé traite ces données avec les secure sketches associés SSi pour obtenir $w''(mod_1),\ldots,w''(mod_n)$, données corrigées et qui vont être utilisées pour déterminer les modalités valides.

Soit L' la liste des modalités valides.

Pour i=1 à n

Si $h'(w''(mod_i))=v_i$, ajouter i dans L'.

Si |L'|<k , on s'arrête.

Sinon, on effectue le partage de secret avec k modalités appartenant à L'.

Supposons que k modalités au moins soient valides et, dans un cas particulier à titre illustratif et non limitatif, que les k premières modalités sont valides : L'={1,…,k}.

a6) Partage de secret

Les données disponibles à ce stade sont les $w_i=w(mod_i)$ valides pour i=1 à k ainsi que la donnée D qui permet d'effectuer le partage de secret obtenue grâce à l'initialisation du secret.

Cas particulier pour les étages E2 et plus

Pour les étages Ei (i>=2) de la cascade, les modalités sont remplacées par les Ki,j et les secure sketches sont supprimés. On utilise directement les Ki,j dans le partage de secret.

Initialisation :

b1) Génération de la clé cryptographique

Soient $w_1=K_{i,1}$, …, $w_n=K_{i,n}$ les clés cryptographiques appartenant au groupe considéré sur l'étage i (ici le groupe i,1 par commodité de notations). Soit L_m la liste des clés $K_{i,j}$ dont on veut que la clé cryptographique en sortie $K_{i+1,1}$ du système dépende. Soit alors la clé cryptographique $K_{i+1,1}=f(L_m)$.

Exemple : pour f(.), on peut par exemple concaténer les w_i pour i dans L_m rangés par ordre croissant puis hacher le tout avec une fonction de hachage h_1.

Si $L_5=\{1, 2, 5, 7, 12\}$, $K = h_1(w_1|| w_2|| w_5|| w_7|| w_{12})$.

Autre exemple : On choisit une fonction de hache h_1, puis pout tout i dans L_m on calcule $h_1(w_i)$. Ensuite, par exemple si $L_5=\{1, 2, 5, 7, 12\}$, on pose $K=f(L_m)=h_1(w_1) \oplus h_1(w_2) \oplus h_1(w_5) \oplus h_1(w_7) \oplus h_1(w_{12})$.

b2) Initialisation du partage de secret

Cette phase a pour but de distribuer le secret $K_{i+1,1}$ entre les différentes clés. Il n'est pas possible d'utiliser directement les schémas

classiques de partage de secret car une partie des morceaux de secret distribués est imposé par les w_i : il faut adapter le partage de secret.
Le partage de secret engendre des données qui doivent être stockée (ces données sont publiques) ; la donnée D contient ces éléments.

b3) Autres données à stocker

Pour le partage de secret, il est nécessaire de savoir quelles clés sont valides afin d'en sélectionner $k_{i+1,1}$ valides. Pour cela on choisit une fonction de hachage h' et on stocke pour i=1 à n les $v_i=h'(w_i)$.

Phase d'utilisation :

b4) Recherche de $k_{i+1,1}$ clés valides

Soit L' la liste des modalités (ici les clés Ki,j) valides. Soient w_i'' les clés cryptographiques obtenues par l'étage supérieur.
Pour i=1 à n

Si $h'(w''_i)=v_i$, ajouter i dans L'.

Si $|L'|< k_{i+1,1}$, on s'arrête.
Sinon, on effectue le partage de secret avec $k_{i+1,1}$ modalités appartenant à L'.

Supposons que $k_{i+1,1}$ modalités au moins sont valides. Sans perte de généralité, nous pouvons supposer que les $k_{i+1,1}$ premières modalités sont valides : $L'=\{1,\ldots, k_{i+1,1}\}$.

b5) Partage de secret

Les données disponibles à ce stade sont les w_i valides pour i=1 à $k_{i+1,1}$ ainsi que la donnée D qui permet d'effectuer le partage de secret. On trouve alors la clé $K_{i+1,1}$.

Schéma de partage de secret de Shamir adapté

La description qui suit est donnée en exemple avec une utilisation du partage de secret de type Shamir connu de l'Homme du métier.

Initialisation

c1) Génération de la clé cryptographique

Soient $w_1=w(mod_1)$, ..., $w_n=w(mod_n)$ des mesures sur les modalités Mod_1 ,... Mod_n. Soit L_m la liste des m modalités dont la clé cryptographique en sortie du système dépend. Soit alors la clé cryptographique $K=f(L_m)$.

Les exemples pour la fonction f sont les mêmes que dans les descriptions précédentes.

c2) Enrôlement des secure sketches

A chaque modalité est associé un secure sketch, on effectue leurs enrôlements avec les données w_1, ...,w_n pour obtenir les sketches $s_1=s(mod_1)$, ..., $s_n=s(mod_n)$.

c3) Initialisation du partage de secret

Dans le cas du schéma de partage de secret de Shamir, le procédé comporte par exemple les étapes suivantes :

Le secret est S = K que l'on doit partager entre n modalités avec un seuil k. Pour cela on effectue les actions suivantes :

- Choisir une fonction de hachage h. On prendra par exemple h = SHA-512.
- Le secret est S=K. On souhaite que le seuil du partage de secret soit k un entier compris entre 2 et n.
- Choisir alors aléatoirement un polynôme $f(x) = S + a_1x + ... + a_{k-1}x^{k-1}$.
- Pour chaque modalité, c'est-à-dire pour i=1,...,n, associer le couple $(h(w_i), f(h(w_i)))$ où $w_i = w(mod_i)$.

On stocke ensuite dans la variable D (donnée publique) les données $f(h(w_i))$, ordonnées des points, pour i=1 à n.

Les points utilisés dans le schéma de partage de secret sont les $(h(w_i), f(h(w_i)))$ alors qu'intuitivement il serait plus facile d'utiliser les $(w_i, f(w_i))$. Cependant, une fois le polynôme retrouvé, il serait possible par

calcul d'antécédents de retrouver les abscisses de tous les points ce qui n'est pas souhaité. Grâce à la fonction h, un calcul d'antécédents ne dévoilera pas d'information sur les w_i.

c4) Autres données à stocker

Pour le partage de secret, il est nécessaire de savoir quelles modalités sont valides afin d'en sélectionner k valides. Pour cela on choisit une fonction de hachage h' et on stocke pour i=1 à n les $v_i=h'(w(mod_i))$.

Remarque : il faut absolument que h' soit une fonction différente de h sinon un attaquant peut avoir accès aux points $(h(w_i),f(h(w_i)))$ et donc retrouver la clé cryptographique K.

Phase d'utilisation

c5) Recherche de k modalités valides

Pour chacune des mesures des n modalités nous obtenons les données $w'(mod_1),\ldots,w'(mod_n)$. On corrige ces données avec les secure sketches pour obtenir $w''(mod_1),\ldots,w''(mod_n)$.

Soit L' la liste des modalités valides.

Pour i=1 à n

Si $h'(w''(mod_i))=v_i$, ajouter i dans L'.

Si |L'|<k , on s'arrête, s'il existe moins de k éléments on peut s'arrêter car il est alors possible de retrouver la clé.

Sinon, on effectue le partage de secret avec k modalités appartenant à L'.

Supposons que k modalités au moins sont valides. Sans perte de généralité, nous pouvons supposer que les k premières modalités sont valides : L'={1,…,k}.

c6) Partage de secret

Les données disponibles à ce stade sont les $w_i=w(mod_i)$ valides pour i=1 à k ainsi que $D = \{f(h(w_i)) \mid i=1 \text{ à } n\}$.

Le recouvrement du secret s'effectue de la façon suivante :

- A partir de D, former les couples $(h(w_1), f(h(w_1)))$, …., $(h(w_k), f(h(w_k)))$.

- En utilisant l'interpolation de Lagrange par exemple, l'essentiel étant de trouver le polynôme de degré minimum qui passe par tous les points ($h(w_i)$, $f(h(w_i))$), retrouver le polynôme f(x) et donc son ordonnée à l'origine S=K (d'autres méthodes d'interpolation sont possibles).

Autres schémas de partage de secret

La description précédente a présenté une utilisation du partage de secret de Shamir. Dans le cas général, il est possible d'utiliser n'importe quel schéma de partage de secret qu'il soit à seuil ou non (dans ce cas k=n).

La description va maintenant donner quelques schémas de partage de secret et expliquer quelles étapes sont mises en œuvre pour les adapter à la présente demande de brevet.

Partage avec des Xor

Dans le cas du partage de secret avec des $\oplus$ (Xor) connu de l'Homme du métier, soit le secret $s \in \{0;1\}^l$. On choisit aléatoirement $s_1,\ldots,s_{n-1}$ dans $\{0;1\}^l$ puis on calcule $s_n = s \oplus s_1 \oplus \ldots \oplus s_{n-1}$. Il ne reste plus qu'à distribuer les s_i. Tous les participants doivent être présents pour retrouver le secret s : on peut voir ce schéma comme un partage de secret dont le seuil est n.

Pour adapter ce schéma à notre invention, on prend s=K, pour i=1 à n on pose $s_i=w(mod_i)$ puis $D = s \oplus s_1 \oplus \ldots \oplus s_n$.

Pour retrouver le secret, les n modalités doivent être valides et on le retrouve en calculant $s = D \oplus w_1 \oplus \ldots \oplus w_n$.

Partage de secret modulaire

Dans ce schéma de partage de secret, qui n'est pas à seuil, le secret $s \in Z_N$ est distribué entre n personnes de la façon suivante :

- pour i=1 à n-1, choisir aléatoirement $s_i \in Z_N$
- calculer $s_n = s - (s_1 + \ldots + s_{n-1}) \bmod N$
- donner à chaque utilisateur i la donnée s_i

En ce qui concerne le recouvrement du secret s, n-1 personnes ne peuvent pas le faire mais n le peuvent aisément en calculant $s = s_1 + ... + s_n \bmod N$

Pour adapter ce schéma à la présente invention, on prend s=K mod N, pour i=1 à n on pose s_i=w(mod$_i$) mod N puis $D = s + s_1 + ... + s_n \bmod N$.

Pour retrouver le secret, les n modalités doivent être valides et le secret est retrouvé en calculant $s = D + w_1 + ... + w_n \bmod N$.

Sans sortir du cadre de l'invention, il est aussi possible d'utiliser des schémas de partages de secret connus de l'Homme du métier, tels que l'application des codes correcteurs au partage de secret. .

Généralisations

Généralisation	description
SS => SSg	On remplace k SS par des secure sketches généralisés SSg (k=1 à n) et pour chaque SS transformé on introduit une clé $S_k^{(i)}$ qui peut être publique ou secrète.
SS => SSgr	On remplace k SS par des SSgr secure sketches généralisés recentrés (k=1 à n) et pour chaque SS transformé on introduit une clé $S_k^{(i)}$ qui peut être publique ou secrète.
Plusieurs clés cryptographiques	Il y a 2^n façons de choisir de quelles modalités dépend la clé et n façons de choisir le seuil k. Il y a en tout $n2^n$ dépendances possibles pour la clé cryptographique. Cette généralisation consiste à créer plusieurs clés cryptographiques (donc plusieurs initialisations et plusieurs valeurs de D). C'est la valeur de D que l'on choisit dans le partage de secret qui déterminera le seuil, la dépendance et donc la clé K en sortie du système.

Application à la biométrie	Les modalités en entrée de l'invention peuvent être modalités biométriques (voix, iris, empreinte, visage…).
Application aux PUFs	Les modalités en entrée de l'invention peuvent être des réponses de PUFs (Physical Unclonable Functions).
Dépendance de K	K dépend de la liste L_m mais peut aussi dépendre de d'autres données extérieures au système.
Invention en cascade	Il est possible d'authentifier les modalités par groupes

Exemple de mise en œuvre du procédé selon l'invention :

On veut authentifier un appareil électronique qui comporte 3 PUFs avec 5 utilisateurs sous la condition qu'au moins 4 utilisateurs soient présents et 2 PUFs soient valides.

Pour cela on va chainer l'invention de la façon suivante :

- On utilise l'invention pour générer une clé Kuser ($K_{1,1}$) qui est retrouvée si au moins 4 des 5 utilisateurs sont présents
- On utilise l'invention une deuxième fois pour générer une clé Kpuf ($K_{1,2}$) qui est retrouvée si au moins 2 PUFs sont valides.
- On utiliser enfin une troisième fois l'invention qui génère une clé K ($K_{2,1}$) lorsque les clés Kuser ($K_{1,1}$) et Kpuf ($K_{1,2}$) sont valides. Cette troisième utilisation ne fait pas intervenir de données floues et n'a pas de seuil, il est donc possible d'utiliser un autre système que cette invention pour cette phase. On peut par exemple calculer K=h(Kuser||Kpuf) qui n'est valide qui si Kuser et Kpuf le sont ou bien utiliser l'invention sans les secure sketches.

Il est, par exemple, possible d'authentifier une radio comportant trois PUFs avec deux utilisateurs à condition qu'au moins quatre des cinq modalités (2 biométries et 3 PUFs) soient valides.

Il est possible de généraliser les exemples précédemment décrits en formant des groupes de modalités pour obtenir un certain nombre de clés puis de combiner ces clés pour en trouver d'autres, etc....

La figure 5 représente un exemple de système selon l'invention comprenant plusieurs capteurs 21 adaptés à mesurer des modalités associées à un ou plusieurs utilisateurs, une unité de calcul ou processeur 20 permettant d'exécuter les étapes du procédé selon l'invention, un support d'enregistrement 23 des éléments ou de la donnée D de partage de secret, une mémoire de stockage 22.

Le procédé et le dispositif selon l'invention peuvent s'appliquer pour de l'authentification de modalités qui peuvent être toutes indépendantes les unes des autres. Les modalités peuvent être toutes sortes de données floutées comme par exemple des mesures biométriques (empreinte, iris, voix, visage, main, ...), des réponses de PUFs et même la combinaison de ces modalités.

Le procédé et le dispositif selon l'invention permettent notamment d'effectuer une authentification multimodale à seuil dont la clé cryptographique en sortie du système dépend de modalités choisies, les modalités n'étant pas nécessairement valides.

Ainsi, la clé cryptographique en sortie du système peut dépendre du nombre de modalités souhaitées par un utilisateur et le seuil d'authentification être quelconque.

Revendications

1 – Procédé pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets, en utilisant un principe d'authentification multimodale avec différentes modalités Modi (i=1 à n) réparties dans différents groupes Gi,j, un groupe étant utilisé pour faire de l'authentification multimodale à seuil d'authentification ki, j avec un schéma de partage de secret, i étant l'indice de l'étage Ei d'une cascade et j l'indice du groupe considéré dans un étage et des multi seuils dans un système d'authentification comportant plusieurs étages de traitement caractérisé en ce qu'il comporte au moins les étapes suivantes

Une phase d'initialisation comprenant au moins

au niveau du premier étage E1 du système :

a1) une première étape consiste à générer une clé cryptographique K en utilisant des mesures $w_1=w(mod_1)$, …, $w_n=w(mod_n)$ sur lesdites modalités Mod_1 ,… Mod_n,

soit L_m la liste des m modalités dont la clé cryptographique en sortie du système dépend, ces modalités et leur nombre sont choisis en fonction d'une application donnée,

soit une donnée $K=f(L_m)$ avec f une fonction dont les propriétés sont telles que la donnée K est non prédictible, le procédé exécute les étapes suivantes

a2) une deuxième étape d'enrôlement des secure sketches en associant à chaque modalité Modi un secure sketch SSi,

a3) une troisième étape d'initialisation du partage de secret en distribuant le secret K entre les différentes modalités Modi, et en générant des données qui sont mémorisées dans une donnée publique D,

a4) une quatrième étape de stockage de données en déterminant

les modalités valides en utilisant une fonction non inversible et en stockant en faisant varier l'indice de l'étage de i=1 à n les valeurs $v_i=h'(w(mod_i))$ obtenues en exécutant la fonction non inversible, où h' est une fonction de hachage,

une phase d'utilisation comprenant au moins

a5) une cinquième étape de recherche de k modalités valides en corrigeant pour chacune des mesures des n modalités correspondant à $w'(mod_1),\ldots,w'(mod_n)$, ces mesures avec les secure sketches associés SSi pour obtenir $w''(mod_1),\ldots,w''(mod_n)$, données corrigées ou non en fonction de la validité de la modalité et qui vont être utilisées pour déterminer les modalités valides et pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets.

2 – Procédé selon la revendication 1 caractérisé en ce que on construit une liste L' de modalités valides en exécutant les étapes suivantes :

Soit L' la liste des modalités valides,

on fait varier l'indice de l'étage i de 1 à n

Si $h'(w''(mod_i))=v_i$, on ajoute l'étage i dans la liste de validité L',

Si $|L'|<k$, il existe moins de K éléments dans la liste, on ne fait plus varier l'indice

sinon, on effectue le partage de secret avec k modalités appartenant à L' et on génère la clé associée à l'étage 1 et à un groupe composé de plusieurs modalités Modi.

3 – Procédé selon la revendication 1 caractérisé en ce que l'on détermine à l'étape a4) les modalités en exécutant une fonction de hachage h' et on stocke pour i=1 à n les $v_i=h'(w(mod_i))$ obtenues grâce à l'exécution de la fonction de hachage.

4 – Procédé selon l'une des revendications 1 à 3 caractérisé en ce que pour les étages de rang i supérieur à 1, disposés après le premier étage E1 de la cascade, le procédé utilise les valeurs des clés cryptographiques Ki,j pour le partage de secret avec i l'indice de l'étage considéré et j l'indice du groupe considéré dans l'étage.

5 – Procédé selon la revendication 4 caractérisé en ce qu'il comporte au moins les étapes suivantes :

Génération de la clé cryptographique pour un groupe Gi,j

soient $w_1=K_{i,1}$, …, $w_n=K_{i,n}$ les clés cryptographiques appartenant à un groupe de l'étage i,

soit L_m la liste des clés $K_{i,j}$ dont la clé cryptographique en sortie $K_{i+1,1}$ du système dépend, soit alors la clé cryptographique $K_{i+1,1}=f(L_m)$,

Initialisation du partage de secret en distribuant le secret $K_{i+1,1}$ entre les différentes clés $K_{i,j,}$

Le stockage des données suivantes

pour le partage de secret, k modalités valides sont définies en choisissant une fonction de hachage h' ou une fonction non inversible et on stocke pour l'indice d'étage de i=1 à n les $v_i=h'(w(mod_i))$,

lors de la phase d'utilisation,

on recherche $k_{i+1,1}$ clés valides en exécutant les étapes suivantes

Soit L' la liste des modalités valides.

faire varier l'indice de l'étage de i=1 à n

Si $h'(w_i)=v_i$, ajouter i dans la liste de validité L',

Si $|L'|< k_{i+1,1}$, il existe moins de K éléments dans la liste, on ne fait plus varier l'indice,

Sinon, effectuer le partage de secret avec $k_{i+1,1}$ modalités appartenant à L',

Soient $k_{i+1,1}$ modalités au moins valides, les données disponibles à ce stade sont les w_i valides ainsi que la donnée D qui permet d'effectuer le

partage de secret et à partir desquelles on trouve alors la clé $K_{i+1,1}$ et on effectue l''authentificatioin.

6– Procédé selon la revendication 1 caractérisé en ce que l'on utilise comme partage de secret le partage de secret de Shamir et en ce qu'il comporte au moins les étapes suivantes :

c1) Génération de la clé cryptographique

Soient $w_1=w(mod_1)$, …, $w_n=w(mod_n)$ des mesures sur les modalités Mod_1 ,… Mod_n, L_m la liste des m modalités dont la clé cryptographique en sortie du système dépend et $K=f(L_m)$ la clé cryptographique,

c2) on effectue les enrôlements des secure sketches avec les données w_1, …, w_n pour obtenir les sketches $s_1=s(mod_1)$, …, $s_n=s(mod_n)$.

c3) on initialise le partage de secret en exécutant les étapes suivantes :

déterminer le secret S = K à partager entre n modalités avec un seuil k

- Choisir une fonction de hachage h,

Le secret est S=K avec un seuil du partage de secret k avec k variant de 2 à n-1,

- Choisir aléatoirement un polynôme $f(x)= S + a_1x + … + a_{k-1}x^{k-1}$,
- Pour chaque modalité, c'est-à-dire pour i=1,…,n, associer le couple $(h(w_i), f(h(w_i)))$ où $w_i = w(mod_i)$,

puis stocker dans la variable publique D, les données $f(h(w_i))$, ordonnées des points, pour i=1 à n,

choisir une fonction de hachage h' et stocker pour i=1 à n les $v_i=h'(w(mod_i))$ utilisées pour déterminer les modalités valides dans le partage de secret, avec h' une fonction différente de h,

Phase d'utilisation du procédé

c4) on recherche k modalités valides

pour chacune des mesures des n modalités $w'(mod_1),…,w'(mod_n)$ on corrige ces données avec les secure sketches pour obtenir $w''(mod_1),…,w''(mod_n)$,

Soit L' la liste des modalités valides,

faire varier l'indice de l'étage de i=1 à n

Si h'(w''(mod$_i$))=v$_i$, ajouter i dans la liste de validité L',

Si |L'|<k ,

il existe moins de K éléments dans la liste, on ne fait plus varier l'indice

Sinon, effectuer le partage de secret avec k modalités appartenant à L',

c5) on exécute le partage de secret

Les données disponibles à ce stade sont les w$_i$=w(mod$_i$) valides ainsi que la donnée publique D = {f(h(w$_i$))}.

Effectuer le recouvrement du secret en exécutant les étapes suivantes :

- à partir de D, former les couples (h(w$_1$), f(h(w$_1$))), ..., (h(w$_k$), f(h(w$_k$))), et
- en utilisant l'interpolation (de Lagrange par exemple) avec ces couples, retrouver le polynôme f(x) et donc son ordonnée à l'origine S=K.

7 – Procédé selon l'une des revendications 1 à 6 caractérisé en ce que pour effectuer l'étape de génération de la clé cryptographique, le procédé comporte au moins les étapes suivantes :

pour f, concaténer les w$_i$ pour i dans L$_m$ rangés par ordre croissant puis utiliser une fonction de hachage h$_1$,

ou choisit une fonction de hachage h$_1$, puis pour tout i dans L$_m$ on calcule h$_1$(w$_i$), puis on additionne les différents éléments de L$_m$ avec l'opération $\oplus$.

8 – Procédé selon l'une des revendications 1 à 6 caractérisé en ce que la fonction de partage de secret utilisée consiste à partager avec des Xor $\oplus$, le secret s$\in$ {0 ;1}^{l}, choisir aléatoirement s$_1$,...,s$_{n-1}$ dans {0 ;1}^{l} puis calculer s$_n$ = s $\oplus$ s$_1$ $\oplus$ ... $\oplus$ s$_{n-1}$, distribuer tous les s$_i$, et adapter ce schéma en prenant s=K puis, pour i=1 à n en posant s$_i$=w(mod$_i$) et $D = s \oplus s_1 \oplus ... \oplus s_n$,

puis retrouver le secret pour les n modalités en calculant $s = D \oplus w_1 \oplus ... \oplus w_n$.

9 – Système pour authentifier un ou plusieurs utilisateurs ou objets, un ou plusieurs utilisateurs conjointement avec un ou plusieurs objets en utilisant un principe d'authentification multimodale avec différentes modalités Modi (i=1 à n) réparties dans différents groupes Gi,j, un groupe étant utilisé pour faire de l'authentification multimodale à seuil ki, j avec un schéma de partage de secret, i étant l'indice de l'étage d'une cascade et i l'indice du groupe considéré dans un étage et des multi seuils caractérisé en ce qu'il comporte au moins les éléments suivants : plusieurs capteurs (21) adaptés à mesurer des modalités associées à un ou plusieurs utilisateurs, une unité de calcul ou processeur (20) permettant d'exécuter les étapes du procédé selon l'une des revendications 1 à 8, des modules de mémorisation des données telles que les secure sketches.

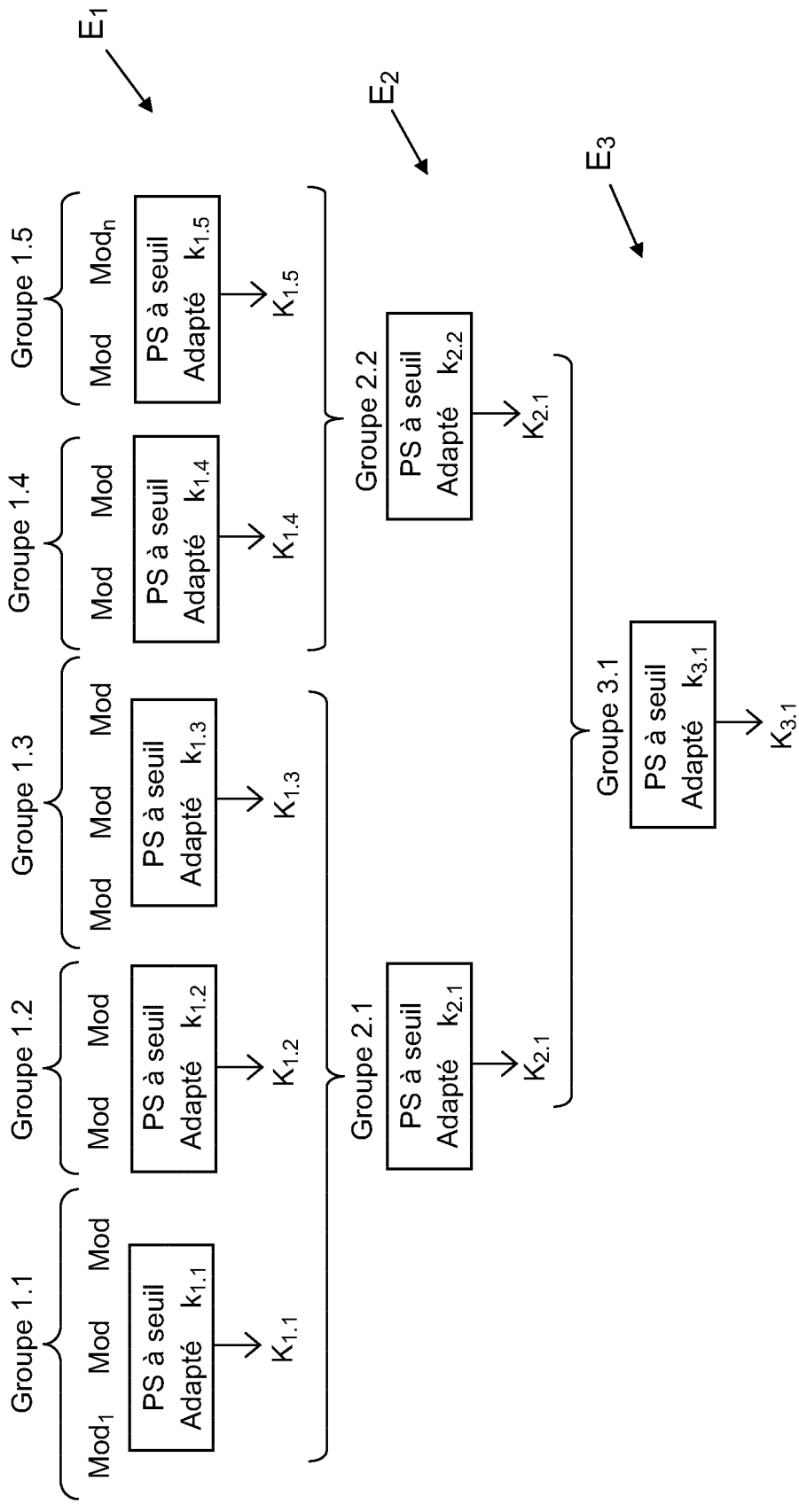

E1
E2
E3
Groupe 1.1
Groupe 1.2
Groupe 1.3
Groupe 1.4
Groupe 1.5
Groupe 2.1
Groupe 2.2
Groupe 3.1
Mod1 Mod Mod
Mod Mod
Mod Mod Mod
Mod Mod
Mod Modn
PS à seuil Adapté k1.1
PS à seuil Adapté k1.2
PS à seuil Adapté k1.3
PS à seuil Adapté k1.4
PS à seuil Adapté k1.5
PS à seuil Adapté k2.1
PS à seuil Adapté k2.2
PS à seuil Adapté k3.1
K1.1
K1.2
K1.3
K1.4
K1.5
K2.1
K2.1
K2.2
K3.1

FIG.1

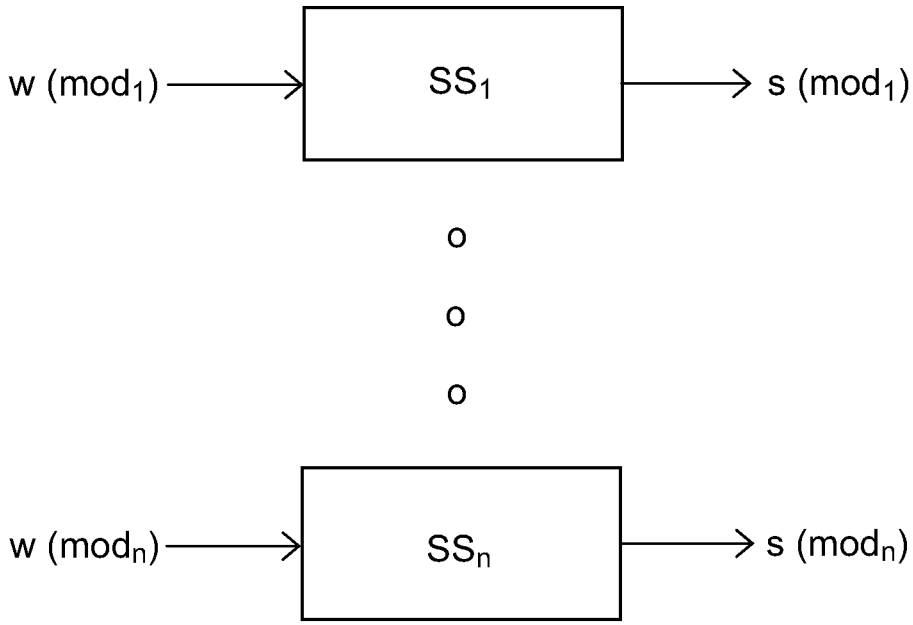

w (mod1)
SS1
s (mod1)
o
o
o
w (modn)
SSn
s (modn)

FIG.2

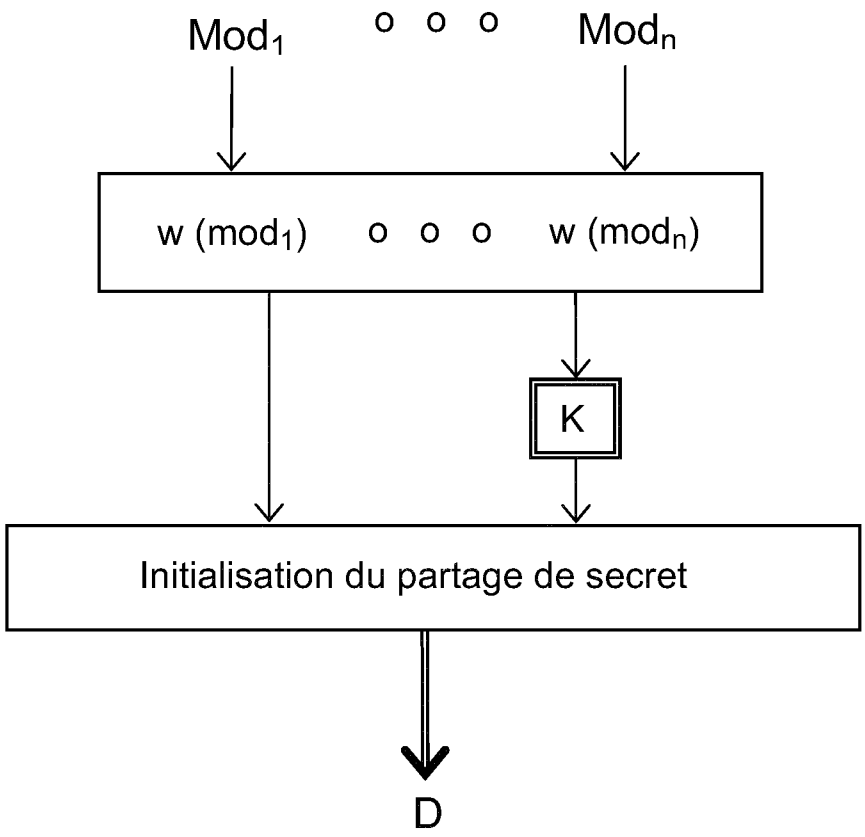

Mod1
o o o
Modn
w (mod1) o o o w (modn)
K
Initialisation du partage de secret
D

FIG.3

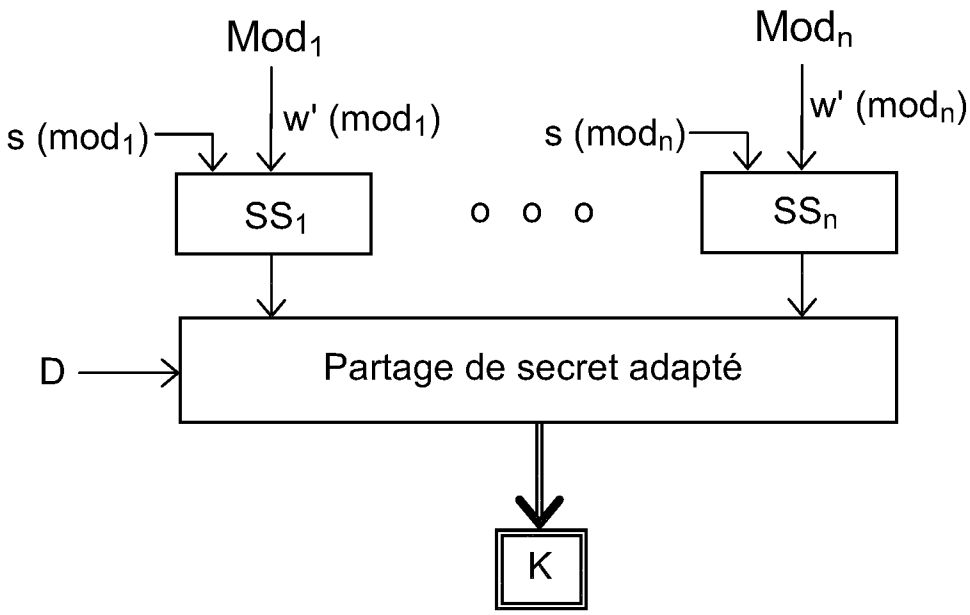

Mod1
Modn
w' (mod1)
w' (modn)
s (mod1)
s (modn)
SS1
o o o
SSn
D
Partage de secret adapté
K

FIG.4

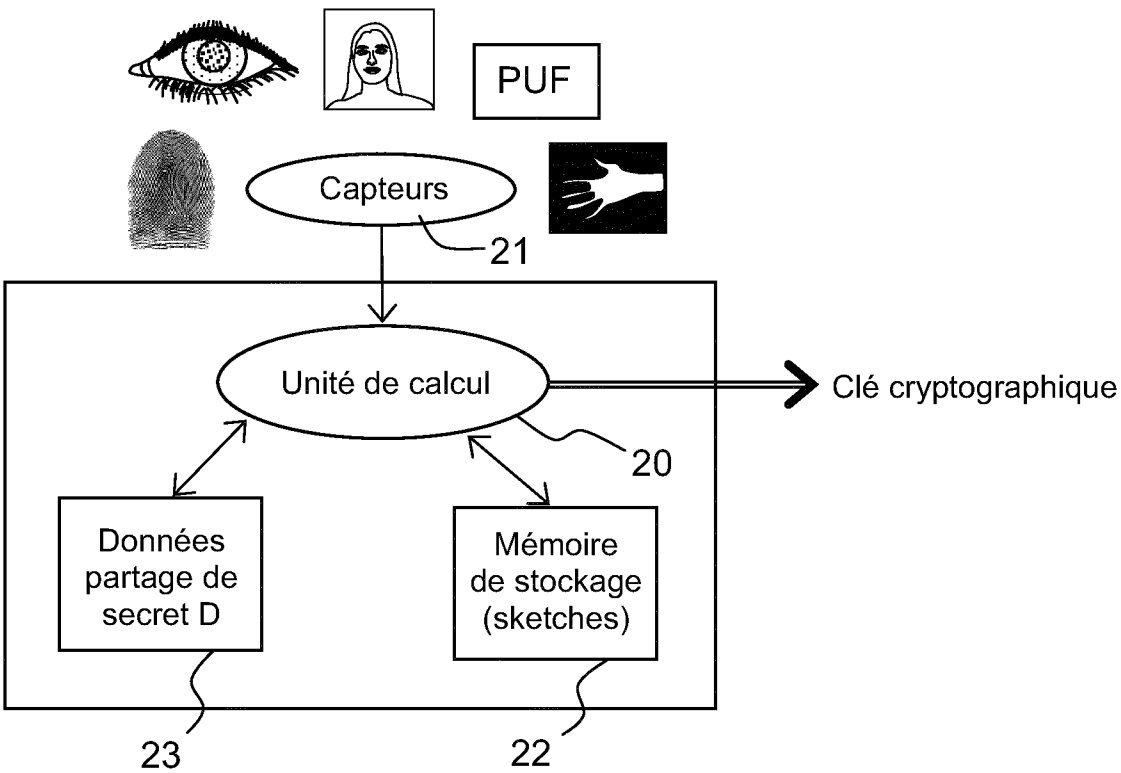

PUF
Capteurs
21
Unité de calcul
Clé cryptographique
20
Données partage de secret D
Mémoire de stockage (sketches)
23
22

FIG.5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/073810

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08
ADD.

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)
H04L

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, PAJ, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2008/010773 A1 (PRIVYLINK PTE LTD [SG]; LAM KWOK YAN KARCH [SG]; HUANG YI YUAN [SG]; S) 24 January 2008 (2008-01-24) page 6, line 1 - line 16 page 9, line 15 - page 13, line 19 page 19, line 4 - page 24, line 15 -----	1-9
A	CHANGLU LIN ET AL: "Ideal Perfect Multilevel Threshold Secret Sharing Scheme", INFORMATION ASSURANCE AND SECURITY, 2009. IAS '09. FIFTH INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 18 August 2009 (2009-08-18), pages 118-121, XP031543915, ISBN: 978-0-7695-3744-3 the whole document ----- -/--	1-9

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

[X] 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	Date of mailing of the international search report
20 February 2012	28/02/2012

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bec, Thierry

1

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/073810

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TAMIR TASSA: "Hierarchical Threshold Secret Sharing", JOURNAL OF CRYPTOLOGY, SPRINGER-VERLAG, NE, vol. 20, no. 2, 6 February 2007 (2007-02-06), pages 237-264, XP019487898, ISSN: 1432-1378, DOI: 10.1007/S00145-006-0334-8 paragraph [0003]	1-9
A	WO 2007/069146 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; TUYLS PIM T [BE]; SCHOENMAKERS BE) 21 June 2007 (2007-06-21) page 2, line 3 - page 3, line 18 page 3, line 3 - line 27 page 5, line 31 - page 7, line 8	1-9

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2011/073810

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2008010773 A1	24-01-2008	AU 2007275938 A1	24-01-2008
		SG 139580 A1	29-02-2008
		US 2009310779 A1	17-12-2009
		WO 2008010773 A1	24-01-2008
WO 2007069146 A2	21-06-2007	CN 101331706 A	24-12-2008
		EP 1964305 A2	03-09-2008
		JP 2009519490 A	14-05-2009
		US 2008304657 A1	11-12-2008
		WO 2007069146 A2	21-06-2007

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2011/073810

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L9/08
ADD.

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)
H04L

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, PAJ, WPI Data, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2008/010773 A1 (PRIVYLINK PTE LTD [SG]; LAM KWOK YAN KARCH [SG]; HUANG YI YUAN [SG]; S) 24 janvier 2008 (2008-01-24) page 6, ligne 1 - ligne 16 page 9, ligne 15 - page 13, ligne 19 page 19, ligne 4 - page 24, ligne 15 -----	1-9
A	CHANGLU LIN ET AL: "Ideal Perfect Multilevel Threshold Secret Sharing Scheme", INFORMATION ASSURANCE AND SECURITY, 2009. IAS '09. FIFTH INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 18 août 2009 (2009-08-18), pages 118-121, XP031543915, ISBN: 978-0-7695-3744-3 le document en entier ----- -/--	1-9

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] 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	Date d'expédition du présent rapport de recherche internationale
20 février 2012	28/02/2012

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Bec, Thierry

1

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	TAMIR TASSA: "Hierarchical Threshold Secret Sharing", JOURNAL OF CRYPTOLOGY, SPRINGER-VERLAG, NE, vol. 20, no. 2, 6 février 2007 (2007-02-06), pages 237-264, XP019487898, ISSN: 1432-1378, DOI: 10.1007/S00145-006-0334-8 alinéa [0003]	1-9
A	WO 2007/069146 A2 (KONINKL PHILIPS ELECTRONICS NV [NL]; TUYLS PIM T [BE]; SCHOENMAKERS BE) 21 juin 2007 (2007-06-21) page 2, ligne 3 - page 3, ligne 18 page 3, ligne 3 - ligne 27 page 5, ligne 31 - page 7, ligne 8	1-9

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2011/073810

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
WO 2008010773 A1	24-01-2008	AU 2007275938 A1	24-01-2008
		SG 139580 A1	29-02-2008
		US 2009310779 A1	17-12-2009
		WO 2008010773 A1	24-01-2008
WO 2007069146 A2	21-06-2007	CN 101331706 A	24-12-2008
		EP 1964305 A2	03-09-2008
		JP 2009519490 A	14-05-2009
		US 2008304657 A1	11-12-2008
		WO 2007069146 A2	21-06-2007