



(51) Classification internationale des brevets :
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2011/073538

(22) Date de dépôt international :
21 décembre 2011 (21.12.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
10/05118 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) : **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). **MARCELLO, Sandra** [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.; Marks & Clerk France, 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, 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))

(54) Title : METHOD OF MULTIMODAL AUTHENTICATION WITH THRESHOLD AND GENERATION OF UNIMODAL KEY

(54) Titre : PROCEDE D'AUTHENTIFICATION MULTIMODALE A SEUIL ET GENERATION DE CLE UNIMODALE

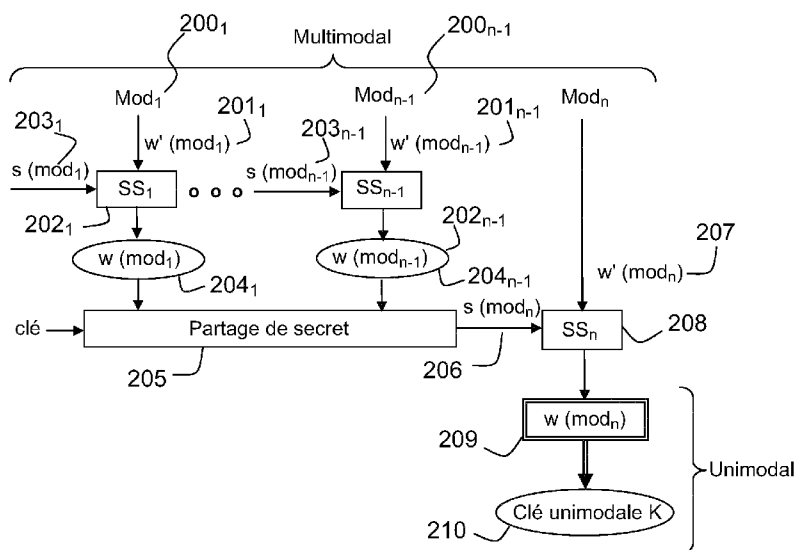


FIG.2

205 Sharing of secret
210 Unimodal key K

(57) Abstract : The invention relates to a method for authenticating one or more users in which sketches $s(mod_i)$ are defined, the "key" to be used for a function for sharing a secret is determined, for each of the modalities Mod_1 to Mod_n , the modality i is measured Mod_i 200i, then said measurement $w'(mod_i)$ is processed 203i using the associated sketch $s(mod_i)$ 202i, the value of $s(mod_n)$ is retrieved 206 on the basis of said known key and on the basis of the (at least) k different values $w(mod_i)$ which are valid and of a function f for sharing a secret 205 so as to reconstruct the sketch $s(mod_n)$ of the modality n , the noisy value of the modality n is measured, so as to obtain $w'(mod_n)$ 207, and said data item is processed so as to retrieve the value $w(mod_n)$, 209, and on the basis of this value $w(mod_n)$, a unimodal cryptographic key K is determined, 210.

(57) Abrégé : L'invention concerne un procédé pour authentifier un ou plusieurs utilisateurs dans lequel

[Suite sur la page suivante]



on définit des sketches $s(\text{modi})$, on détermine la "clé" à utiliser pour une fonction de partage de secret, pour chacune des modalités Mod1 à Modn-1 , on mesure la modalité i , Modi 200i, puis on traite ladite mesure $w'(\text{modi})$ 203i en utilisant le sketch associé $s(\text{modi})$ 202i, on retrouve la valeur de $s(\text{modn})$ 206 à partir de ladite clé connue et à partir des (au moins) k différentes valeurs $w(\text{modi})$ valides et d'une fonction f de partage de secret 205 afin de reconstruire le sketch $s(\text{modn})$ de la modalité n , on mesure la valeur bruitée de la modalité n , afin d'obtenir $w'(\text{modn})$ 207, et on traite ladite donnée afin de retrouver la valeur $w(\text{modn})$, 209, et à partir de cette valeur $w(\text{modn})$ on détermine une clé cryptographique unimodale K , 210.

PROCEDE D'AUTHENTIFICATION MULTIMODALE A SEUIL ET GENERATION DE CLE UNIMODALE

L'objet de l'invention concerne notamment un procédé permettant
5 d'authentifier un ou plusieurs utilisateurs ou objets à partir de plusieurs modalités.

Le terme « modalité » est utilisé dans la présente description pour désigner une donnée biométrique associée à un individu, un PUF associé à un objet ou tout autre type de données floues que l'on souhaite authentifier.
10 Un PUF (Physical Unclonable Function) est, par exemple, une fonction réalisée sur un circuit électronique qui envoie des challenges et reçoit les réponses. La sortie du PUF correspond à une ou plusieurs de ces réponses. Les « challenges » sont basés sur des éléments physiques aléatoires choisis de telle sorte qu'un PUF donnera des réponses similaires sur un même
15 circuit et des réponses différentes sur deux circuits distincts. On utilise par exemple le temps de parcours sur des chemins différents, l'initialisation des transistors, des propriétés optiques...

Les réponses peuvent faire office de modalités pour authentifier des composants sur des circuits électroniques.

20 Le mot « donnée biométrique », dans la suite de la description, couvre les empreintes digitales, l'iris, ... 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,
- 25 • d'une ou plusieurs personnes grâce à la biométrie multimodale,
- de la combinaison de supports et de personnes,
- 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 biométrique ou
30 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 :

5 l'identification et l'authentification, et la génération de clés cryptographiques.

Le problème posé correspond à authentifier plusieurs modalités dont une a été définie comme principale.

Un exemple de critère permettant de définir la modalité principale est de considérer celle dont la sécurité lors de son utilisation dans un secure sketch est parfaitement maîtrisée. Un secure sketch est défini plus précisément

10 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 » Eurocrypt 2004, LNCS, vol 3027, pp 523-540 qui traite du problème du caractère non uniforme des données mesurées et de la

15 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

20 rétablissement d'une valeur systématiquement identique en sortie pour une même donnée d'entrée avec un bruit suffisamment faible, 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

25 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

30 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
 5 de la mesure confidentielle de référence w à partir d'une donnée bruitée w' .

Les figures 1A et 1B schématisent respectivement la phase d'enrôlement et la phase de recouvrement. Sur ces figures, w est la donnée d'origine, s est le sketch, et w' la seconde donnée floue ou bruitée.

Plus formellement, dans l'article précité, un secure sketch est défini de la
 10 façon suivante : soit M correspondant à un espace métrique muni d'une distance entre w et w' qui sont des mesures des données et m, m' des paramètres d'entropie ; un secure sketch de paramètres (M, m, m', t) est une paire de procédures 'sketch' ou enrôlement (Enrol) et 'recover' ou recouvrement (Rec) telles que :

- 15 1. La procédure Enrol 100 prend en entrée $w \in M$ et retourne une chaîne de bits $s \in \{0;1\}^*$.
2. La procédure de recouvrement Rec 101 prend en entrée un élément $w' \in M$ et une chaîne de bits $s \in \{0;1\}^*$. La propriété de correction du secure sketch garantit que si $\text{dis}(w, w') \leq t$ alors $\text{Rec}(w', \text{SS}(w)) = w$. Si $\text{dis}(w, w') > t$,
 20 aucune garantie n'est donnée sur la sortie de Rec.
3. La propriété de sécurité garantit que pour toute distribution W sur M de min-entropie m , la valeur de w ne peut être retrouvée par l'adversaire qu'avec une probabilité inférieure à $2^{-m'}$: $\bar{H}_\infty(W, \text{SS}(W)) \geq m'$ où $\bar{H}_\infty(.)$ est la min-entropie..

25

Comme expliqué précédemment, 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
 30 de référence w est la donnée caractéristique obtenue par une première

mesure de cette empreinte par un capteur. Par la suite, la phase de correction est exécutée à chaque fois que l'on souhaite retrouver la donnée de référence w . A cette fin, une donnée bruitée w' provenant d'une mesure issue d'un traitement de la donnée confidentielle W – par exemple, une
5 seconde mesure de la même empreinte digitale – est combinée à la donnée publique s . La donnée publique s joue donc un rôle dans la reconstruction de la mesure confidentielle de référence w à partir d'une donnée bruitée w' . Si la donnée bruitée w' est trop éloignée de la donnée de référence w , cette donnée de référence w ne peut être reconstruite. C'est le cas, par exemple,
10 lorsque la donnée bruitée w' est obtenue par une mesure d'un traitement d'une donnée X différente de la donnée confidentielle W .

L'un des problèmes de l'art antérieur est que les solutions proposées ne permettent pas l'interopérabilité des différents types de modalités utilisées et que la sécurité repose sur le maillon qui possède la
15 sécurité la plus faible.

Les solutions biométriques multimodales connues du Demandeur utilisent la combinaison des solutions dédiées à chaque type de biométrie.

Ainsi, l'art antérieur ne lie pas les secure sketches entre eux pour effectuer de l'authentification multimodale. Le problème résolu généralement
20 dans l'art antérieur est de faire de l'authentification multimodale pour en déduire une clé multimodale, mais dans la plupart des cas, notamment dans le cas d'utilisation de PUFs, on maîtrise la sécurité de certains PUFs mais pas complètement ou nécessairement celle des autres.

L'un des problèmes posés dans la présente demande de brevet
25 est de faire de l'authentification multimodale sur les modalités dont la sécurité n'est pas complètement maîtrisée à ce jour et d'en déduire une clé unimodale qui dépend de la modalité principale. Dans les applications envisagées la sécurité est le critère qui permet de déterminer la modalité dominante ou principale, rien n'empêche pour un autre type d'application
30 d'utiliser un autre critère pour déterminer la modalité principale.

Le document de Stelvio Cimato et al intitulé « Privacy-Aware Biometrics : Design and Implementation of a Multimodal Verification System », Computer Security applications conference 2008, ACSAC 2008, pages 130-139, XP031376769 décrit un système mettant en œuvre des
5 secure sketches où les différents modules d'authentification sont combinés tels quel.

La demande de brevet WO 2008/010773 divulgue un système de génération de clés à partir de données biométriques mettant en œuvre un système à seuil.

10 Le document de Voloshynovsky S et al intitulé « Multimodal authentication based on random projections and source coding », 22 septembre 2008 pages 1-10, XP007919567 décrit l'impact de la présence de modalités additionnelles sur la performance de l'authentification.

Dans la suite de la description, les références suivantes seront
15 utilisées :

- Mod i ou modi : la modalité d'indice i
- $s(\text{modi})$: sketch de la modalité modi qui est obtenu en mesurant la modalité modi et en la soumettant au secure sketch SSi
- SSi : secure sketch i
- 20 • $w(\text{modi})$: mesure de la modalité i
- $w'(\text{modi})$: mesure bruitée de la modalité i
- la fonction f est associée au partage de secret.

L'objet de la présente invention concerne un procédé pour authentifier un ou plusieurs utilisateurs ou objets, voire conjointement un ou
25 plusieurs utilisateurs ou objets en utilisant un principe d'authentification multimodale,

- a) phase d'initialisation : définir les valeurs des sketches $s(\text{modi})$ pour chacune des modalités modi utilisées pour l'authentification, et déterminer la valeur de la donnée « clé » à utiliser pour une fonction de partage de secret,
- 30 b) phase de correction : pour chacune des modalités $\text{mod}1$ à $\text{mod}n-1$, ledit procédé comporte au moins les étapes suivantes :

b1) une étape de mesure de modalité i , Mod_i , ce qui correspond à $w'(mod_i)$, puis une étape de traitement de la mesure $w'(mod_i)$ en utilisant le sketch associé $s(mod_i)$, on authentifie ainsi la donnée mod_i avec le secure sketch SS_i pour obtenir la donnée $w(mod_i)$ qui ne dépend que de Mod_i ,

5 b2) ces étapes sont exécutées pour toutes les modalités i choisies, i allant de 1 à $n-1$,

b3) l'étape suivante consiste à retrouver la valeur du sketch $s(mod_n)$ de la modalité n à partir de ladite donnée clé connue et à partir des différentes valeurs $w(mod_i)$ et d'une fonction f de partage de secret, puis

10 b4) mesurer la valeur bruitée de la modalité n , c'est-à-dire obtenir $w'(mod_n)$ 207, cette valeur étant ensuite traitée en utilisant le sketch $s(mod_n)$ 206 et le secure sketch SS_n afin de retrouver la valeur $w(mod_n)$,

b5) à partir de cette valeur $w(mod_n)$, déterminer une clé cryptographique unimodale K .

15 selon un mode de réalisation, la phase a) d'initialisation comporte au moins les étapes suivantes :

- effectuer des mesures de non bruitée $w(mod_i)$ et exécuter un secure sketch associé dans sa phase d'enrôlement afin d'obtenir le sketch $s(mod_i)$,
- 20 • mémoriser les $n-1$ premiers sketches $s(mod_i)$ dans une mémoire,
- pour trouver la valeur de « clé », utiliser les différentes valeurs mesurées $w(mod_i)$ pour chacune des modalités, une fonction f de partage de secret et la valeur de sketch pour la modalité n : $s(mod_n)$.

Le procédé utilise, par exemple, une fonction de partage de secret à seuil. Tout schéma de partage de secret peut être vu comme un schéma de partage de secret à seuil au besoin avec un seuil égal au nombre total des modalités utilisées avec le partage de secret.

Lors de la phase d'initialisation, la valeur de clé est obtenue à partir des $n-1$ premières modalités, du sketch $s(mod_n)$ et du schéma de partage de secret de Shamir de la manière suivante :

- Choisir une fonction de hachage h avec $h = \text{SHA-512}$.

- Le secret étant $S=s(\text{mod}_n)$, établir un seuil du partage de secret k compris entre 2 et $n-1$,
- Choisir alors aléatoirement un polynôme $f(x)= S + a_1x + \dots + a_{k-1}x^{k-1}$
- Pour chaque modalité, c'est-à-dire pour $i=1,\dots,n-1$, associer le couple $(h(w_i), f(h(w_i)))$ où $w_i = w(\text{mod}_i)$
- Calculer pour $i=1$ à $n-1$, $V_i = h'(w_i)$ où h' est une fonction de hachage,
- Dans clé, stocker $f(h(w_1)), \dots, f(h(w_{n-1}))$ et $V_1,\dots,V_{n-1}$.

Lors de la phase de correction, ledit procédé comporte au moins les étapes suivantes :

à partir des $n-1$ premières modalités, retrouver en se servant des $s(\text{mod}_i)$, $i=1,\dots,n-1$ et de la clé la valeur de $s(\text{mod}_n)$.

- Soient au moins k modalités valides avec un seuil du partage de secret égal à k . Utiliser les V_i contenus dans clé pour trouver les modalités valides en comparant V_i au haché par h' de la donnée w_i trouvée. Si plus de k modalités sont valides il est suffisant d'en utiliser k choisies par exemple aléatoirement ou par ordre d'apparition parmi les modalités valides. Il est néanmoins possible d'utiliser plus de modalités valides.
- A partir de la donnée clé de la phase d'initialisation, former les couples $(h(w_1), f(h(w_1))), \dots, (h(w_k), f(h(w_k)))$,
- En utilisant l'interpolation de Lagrange avec ces couples, retrouver le polynôme $f(x)$ et donc son ordonnée à l'origine $S=s(\text{mod}_n)$.

retrouver $w(\text{mod}_n)$ à partir de la dernière modalité ainsi que de $s(\text{mod}_n)$.

Le procédé peut utiliser une fonction de hachage par exemple la fonction de hachage SHA-256 sur la donnée $w(\text{mod}_n)$ pour obtenir la clé cryptographique $K : K=\text{SHA-256}(w(\text{mod}_n))$

La fonction de partage de secret peut être réalisée par une fonction « XOR » lorsque l'on utilise deux modalités et que les tailles de $s(\text{mod}_2)$ et $w(\text{mod}_1)$ sont choisies identiques.

L'invention concerne aussi un dispositif pour authentifier un ou plusieurs utilisateurs ou objets, voire conjointement avec un ou plusieurs objets ou personnes en utilisant un principe d'authentification multimodale caractérisé en ce qu'il comporte en combinaison des moyens d'exécution
5 des étapes du procédé présentant l'une des caractéristiques précitées, des moyens de mesure d'une ou plusieurs modalités associées à un ou plusieurs utilisateurs et des moyens de mémorisation.

D'autres caractéristiques et avantages du dispositif selon l'invention apparaîtront mieux à la lecture de la description qui suit d'un
10 exemple de réalisation donné à titre illustratif et nullement limitatif annexé des figures qui représentent :

- Les figures 1A et 1B schématisent respectivement les phases d'enrôlement et de recouvrement,
- La figure 2, un schéma de fonctionnement du procédé selon
15 l'invention,
- La figure 3, un détail de la phase d'initialisation,
- La figure 4, la phase de correction d'un exemple du procédé selon l'invention en utilisant deux modalités et un schéma de partage de secret avec des Xor,
- 20 • La figure 5, la phase d'initialisation correspondant à la figure 4,
- La figure 6, un exemple d'application mettant en œuvre n secure sketches en série et utilisant des schémas de partage de secret avec des Xor,
- La figure 7, un exemple de phase d'initialisation du schéma de la
25 figure 6,
- La figure 8, une variante pour n secure sketches en parallèle,
- La figure 9, une variante de mise en œuvre de la figure 2 mettant en œuvre des fonctions de hachage, et
- La figure 10 un exemple de système permettant la mise en œuvre du
30 procédé selon l'invention.

Le procédé d'authentification selon l'invention repose notamment sur l'association d'un secure sketch avec une authentification multimodale. C'est-à-dire que l'authentification multimodale permet de retrouver la valeur du sketch associé au secure sketch SS_n via une fonction f . La clé
5 cryptographique est donc unimodale car la sortie du système ne dépend que de la modalité en entrée du dernier secure sketch (la modalité principale), l'authentification multimodale n'est utilisée dans un fonctionnement normal du procédé que pour permettre la correction de la donnée floutée dans le secure sketch (SS_n).

10 La fonction f qui va être utilisée est basée sur un schéma de partage de secret tel que le schéma de partage de secret de Shamir connu de l'Homme du métier qui permet de retrouver le sketch du secure sketch à partir des $n-1$ premières modalités. La fonction f effectuée entre les sorties des traitements des modalités et le SS permet l'association de toutes les
15 modalités en utilisant des protocoles de partage de secret connus de l'Homme du métier. Elle constitue donc un élément majeur de la solution proposée.

La figure 2 représente le schéma global du procédé selon l'invention, on peut la considérer en deux parties : la partie gauche relative
20 aux modalités $Mod_1, \dots, Mod_{n-1}$, et la partie de droite qui comprend le traitement de la modalité Mod_n .

Les valeurs des sketches $s(mod_i)$ pour chacune des modalités mod_i sont par exemple obtenues lors d'une phase d'initialisation précisée à la figure 3.

25 Pour chacune des modalités Mod_1 à Mod_{n-1} , le procédé comporte par exemple les étapes suivantes :

Une étape de mesure de modalité i , Mod_i 200*i*, ce qui correspond à $w'(mod_i)$ 201*i*, puis une étape de traitement de la mesure $w'(mod_i)$ 203*i* en utilisant le sketch associé $s(mod_i)$ 202*i*. On authentifie ainsi la donnée mod_i
30 avec le secure sketch SS_i pour obtenir la donnée $w(mod_i)$ 204*i* qui ne dépend que de mod_i .

Ces étapes 200i à 204i sont exécutées pour toutes les modalités i choisies, de 1 à n-1.

L'étape suivante consiste à retrouver la valeur de $s(\text{modn})$ 206 à partir d'une donnée que l'on appelle « clé » connue et à partir des différentes
5 valeurs $w(\text{modi})$ et d'une fonction f de partage de secret 205 connue de l'Homme du métier. Ceci permet de reconstruire le sketch $s(\text{modn})$ de la modalité n.

Le procédé mesure la valeur bruitée de la modalité n, c'est-à-dire qu'il obtient $w'(\text{modn})$ 207, qu'il traite ensuite utilisant le sketch $s(\text{modn})$ 206
10 et le secure sketch SS_n afin de retrouver la valeur $w(\text{modn})$, 209.

A partir de cette valeur $w(\text{modn})$, le procédé va déterminer une clé cryptographique unimodale K, 210.

La figure 3 représente un exemple d'étapes mises en œuvre pour la phase d'initialisation, effectuée avant utilisation du procédé selon
15 l'invention. Elle permet d'effectuer les phases d'enrôlement des secure sketches ainsi que la distribution des secrets dans le partage de secret 205 et de générer une donnée « clé » qui sera utilisée pour la reconstruction du sketch $s(\text{mod}_n)$ lors de l'application du schéma de partage de secret.

Sur la figure 3, la valeur mesurée non bruitée $w(\text{modi})$ 300i est
20 traitée par le secure sketch dans sa phase d'enrôlement associé 301i afin d'obtenir le sketch $s(\text{modi})$ 302i qui va être utilisé lors des étapes d'authentification et de génération de clé selon l'invention. Pour chacun des secure sketches SS_i , la phase d'enrôlement est effectuée afin de connaître leurs sketches $s(\text{modi})$. Les n-1 premiers sketches $s(\text{modi})$ ainsi obtenus
25 seront stockés dans une mémoire du dispositif selon l'invention. Le dernier sketch $s(\text{modn})$ sert au niveau du partage de secret pour trouver la valeur de la donnée clé en utilisant les différentes valeurs mesurées $w(\text{modi})$ pour chacune des modalités 1 à n-1 et une fonction f de partage de secret. Cette clé permet notamment au partage de secret de fonctionner et ne révèle pas
30 d'informations sensibles ou confidentielles.

Différentes fonctions de partage de secret peuvent être utilisées pour la mise en œuvre du procédé selon l'invention.

Le schéma de partage de secret sera dit « à seuil » dans le cas où le procédé permet qu'au moins k modalités parmi les $n-1$ soient valides pour
5 que l'authentification soit un succès

Le cas extrême où $k=n-1$ correspond à un schéma de partage de secret sans seuil, c'est-à-dire que l'on souhaite que toutes les modalités soient valides pour que l'authentification réussisse. Il peut également être vu comme un partage de secret à seuil égal à $n-1$.

10 Un exemple de schéma de partage de secret connu de l'Homme du métier est celui de Shamir décrit dans l'article intitulé « *How to Share a Secret* » Communications of the ACM, 22:612–613, Nov. 1979.

Définition formelle

15 Le principe proposé par Shamir se base sur l'interpolation polynômiale : étant donnés k points dans un plan de coordonnées $(x_1, y_1), \dots, (x_n, y_n)$, avec $\forall i, j \quad x_i \neq x_j$, il existe un unique polynôme $q(x)$ de degré $k-1$ tel que $\forall i \quad q(x_i) = y_i$.

Soit D le secret que l'on veut partager en sous-secrets D_i . Choisir
20 un polynôme aléatoirement de degré $k-1$ avec $a_0 = D$, $q(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$ puis évaluer $D_1 = q(x_1), \dots, D_n = q(x_n)$.

Etant donnés (au moins) k éléments dans l'ensemble des D_i , par interpolation il est possible de retrouver les coefficients de $q(x)$ et donc la valeur du secret D . La connaissance de seulement $k-1$ éléments ne permet
25 de retrouver aucune information sur la valeur du secret D .

Remarque, il est aussi possible de choisir p un nombre premier et de travailler dans $\mathbb{Z}/p\mathbb{Z}$.

Le principe du schéma de partage de secret de Shamir est qu'il existe un secret et n utilisateurs. Chacun des n utilisateurs reçoit une part du
30 secret et le partage de secret permet de retrouver le secret initial uniquement dans le cas où au moins k utilisateurs mettent leurs parts de secret en

commun; s'ils ne sont que $k-1$ ou moins, ils ne pourront pas obtenir d'information sur le secret.

Plus concrètement, Shamir explique que 2 points suffisent à décrire complètement une droite, 3 pour une parabole, etc. Il faut donc k points pour définir un polynôme de degré $k-1$. Supposons que le secret est S dans un corps F . Il faut alors choisir $k-1$ éléments aléatoirement dans F : $a_1; \dots; a_{k-1}$ et poser $a_0 = S$. Nous construisons ensuite le polynôme $f(x) = a_0 + a_1x + \dots + a_{k-1}x^{k-1}$. Il ne reste plus qu'à donner à chaque utilisateur un couple $(i; f(i))$. Pour retrouver le secret S , il suffit que (au moins) k utilisateurs mettent leurs couples en communs pour retrouver le polynôme et donc le secret. Pour cela, il est par exemple possible d'utiliser les polynômes interpolateurs de Lagrange.

Dans un cas un peu plus général, le partage de secret à seuil peut être défini de la manière suivante

Définition : (partage de secret à seuil k -parmi- n)

Soient k et n deux entiers tels que $0 < k \leq n$. Un partage de secret à seuil k -parmi- n est une méthode de distribution d'un secret $s \in \{0; 1\}^l$ en n morceaux $s_1, \dots, s_n$ telle que pour tout sous-ensemble $S \in \{1; \dots; n\}$:

- si $|S| \leq k$, pour toute machine polynomiale A , en l et n , et pour tout ε non-négligeable, $P_{b \in \{0; 1\}, c \in \{0; 1\}^l} [A((s_i)_{i \in S}, x_0, x_1) = b \mid x_b = s, x_{b=c} = c] < 1/2 + \varepsilon$.
- Si $|S| > k$, il existe une machine polynomiale A telle que : $s = A((s_i)_{i \in S})$.

D'autres schémas de partage de secret sont connus de l'art antérieur, dont certains vont être donnés à titre illustratif et nullement limitatif.

Par exemple, il est possible d'utiliser le partage avec des Xor connu de l'Homme du métier : le secret $s \in \{0; 1\}^l$, choisir aléatoirement $s_1, \dots, s_{n-1}$ dans $\{0; 1\}^l$ puis calculer $s_n = s \text{ Xor } s_1 \text{ Xor } \dots \text{ Xor } s_{n-1}$. Il ne reste plus qu'à distribuer les s_i . Tous les participants doivent être présents pour retrouver le secret s (ce n'est pas un partage de secret à seuil).

Une autre manière de procéder consiste à utiliser un partage de secret modulaire décrit dans ce même document: on travaille ce coup-ci dans $\mathbb{Z}/n\mathbb{Z}$ et $s_n = s - (s_1 + \dots + s_{n-1}) \bmod n$ (n'est pas non-plus un partage de secret à seuil).

5 Quelques exemples de mise en œuvre du procédé selon l'invention vont maintenant être donnés en relation avec les figures 4 à 8.

La figure 4 schématise le cas d'utilisation de deux secure sketches en utilisant un Xor pour le schéma de partage de secret.

La phase de correction comporte au moins les étapes décrites ci-
10 après.

Une première étape consiste en une mesure de la modalité mod1 pour obtenir la valeur bruitée $w'(\bmod 1)$ et, en utilisant le sketch $s(\bmod 1)$ et le secure sketch SS1, à retrouver la valeur de la donnée $w(\bmod 1)$. Le sketch $s(\bmod 2)$ est obtenu à partir de la valeur $w(\bmod 1)$ et de la donnée notée
15 « clé ». Ensuite le sketch $s(\bmod 2)$ sera utilisé pour traiter la valeur $w'(\bmod 2)$ via l'utilisation du secure sketch SS2 afin d'obtenir la donnée $w(\bmod 2)$ qui permettra d'exécuter l'étape d'authentification.

La sortie d'un tel système ne dépend que de la modalité 2 et, si la modalité 1 n'est pas valide, il est impossible de « déflouter » la modalité 2 car
20 le sketch $s(\bmod 2)$ ne peut être retrouvé que si $w(\bmod 1)$ est correct.

Un des avantages est que s'il est nécessaire que la modalité 2 soit plus importante que la première, il est possible de conserver l'authentification de la modalité 2 et changer la modalité 1 sans modifier la sortie du système ($w(\bmod 2)$) : il suffira de stocker des valeurs différentes de $s(\bmod 1)$ et de clé
25 en réalisant une nouvelle initialisation.

Si l'on considère un exemple dans le cadre de la biométrie, la modalité importante ou dont la sécurité du SS qui fait l'authentification est parfaitement maîtrisée, à savoir la modalité 2, est une mesure de l'empreinte digitale qui est associée à une modalité d'importance moindre (modalité 1)
30 qui est par exemple la voix. A partir de la donnée $w(\bmod 2)$ une clé cryptographique est ensuite générée.

S'il est décidé ensuite que la voix n'est pas appropriée pour le type d'authentification effectuée, la modalité mod1 peut représenter l'iris de la personne. Au niveau du procédé, il est alors nécessaire d'effectuer une nouvelle initialisation partielle pour trouver la nouvelle valeur de $s(\text{mod1})$ puis la nouvelle valeur de clé. La valeur de $s(\text{mod2})$ reste inchangée. Le scan de l'iris qui correspond à la mesure de la modalité 1 permet de retrouver avec la clé, la valeur de $s(\text{mod2})$ puis la mesure de l'empreinte digitale permet de retrouver $w(\text{mod2})$ puis la valeur de la clé cryptographique K.

La clé cryptographique K associée à la personne reste inchangée, même si les biométries ou modalités utilisées sont différentes pour effectuer l'authentification.

La figure 5 représente un exemple d'initialisation avec des modalités et un partage de secret utilisant les Xor. Cette dernière doit notamment fournir les sketches des modalités à utiliser et la clé. Pour cela, une façon de procéder consiste à effectuer une mesure de $s(\text{mod1})$ en utilisant la première modalité mod1 puis, pour trouver la clé, le procédé va commencer par calculer $s(\text{mod2})$ puis en détruire la valeur de clé correspondante avec le partage de secret.

La figure 6 schématise une généralisation de la figure 4 avec n secure sketches en série pour la phase de correction, dans lequel il y a (n-1) xor utilisés et l'utilisation de plusieurs clés (clé i). La figure 7, la phase d'initialisation correspondante.

Dans les exemples décrits aux figures 4 à 8, sans sortir du cadre de l'invention, il est possible d'utiliser en lieu et place d'un XOR un partage de secret choisi par exemple parmi ceux cités précédemment.

La figure 8 représente un exemple de mise en œuvre du procédé selon l'invention pour la phase de correction dans lequel il y a un secure sketch central qui va être utilisé pour définir les n-1 clés utilisées par le procédé.

La phase d'initialisation du système de la figure 8 est semblable à la phase d'initialisation décrite à la figure 7, excepté le fait que les différentes

clés $clé_1, \dots, clé_{n-1}$ sont déterminées dans ce cas en utilisant toujours la valeur de la modalité 1, à savoir $w(\text{mod}1)$.

Sans sortir du cadre de l'invention, en lieu et place des secure sketches il est possible d'utiliser des secure sketches généralisés tels que ceux décrits dans la demande de brevet du Demandeur FR09/03699 ou bien des secure sketches généralisés recentrés décrits dans la demande de brevet du Demandeur intitulée « Procédé de reconstruction d'une mesure de référence d'une donnée confidentielle à partir d'une mesure bruitée de cette donnée, notamment pour la génération de clés cryptographiques ».

La figure 9 schématise un exemple de mise en œuvre dans laquelle les secure sketches sont remplacés par des extracteurs flous, par exemple en ajoutant une fonction de hachage h_i à la sortie du secure sketch i . Dans ce cas, il est possible d'utiliser directement la donnée $h(wod(\text{mod}n))$ comme clé cryptographique.

Il est possible de ne remplacer que k secure sketches par des extracteurs flous.

Application aux PUFs (Physical Unclonable Functions)

Un PUF est une fonction réalisée par exemple sur un circuit électronique qui envoie des challenges et reçoit les réponses, plus généralement elle dépend d'une structure physique. La sortie du PUF correspond à une ou plusieurs de ces réponses. Ces challenges sont basés sur des éléments physiques aléatoires choisis de telle sorte qu'un PUF donnera des réponses similaires sur un même circuit et des réponses différentes sur deux circuits distincts. On utilise par exemple le temps de parcours sur des chemins différents, l'initialisation des transistors, des propriétés optiques...

Ces réponses peuvent faire office de modalités pour authentifier des composants sur des circuits électroniques.

Application à la biométrie

Les modalités en entrée des secure sketches peuvent sans problème être des données biométriques comme par exemple la voix, les

empreintes digitales, l'iris, la rétine, le visage... On peut par exemple authentifier une unique personne en mesurant plusieurs de ses données biométriques mais on peut aussi authentifier plusieurs personnes simultanément grâce à ce système. De plus, notre solution permet d'avoir
5 une modalité biométrique principale avec la possibilité de changer facilement les autres modalités.

Il est aussi important de se rendre compte que dans ce genre de cas on utilise des données qui sont de différentes tailles ainsi que différentes métriques ce qui implique l'emploi codes correcteurs différents.

10 **Application aux mots de passe**

Les deux principaux types de modalités que nous utilisons sont les données biométriques et les réponses de PUFs mais nous pourrions en citer une troisième qui est de faire retenir un mot de passe très long à l'utilisateur. La modalité sera ce mot de passe, flouté car l'utilisateur ne se souvient pas
15 exactement de la totalité du mot de passe.

Il est aussi possible de lui faire retenir une liste (d'objets, de films...) et lui demander de la restituer pour former la modalité. Ensuite, nous utilisons la distance symétrique pour comparer à la liste initiale.

Exemple chiffré avec le partage de secret de Shamir

20 Phase d'initialisation

Etape n°1 :

Il y a n modalités à authentifier. Ces modalités peuvent être de tailles et de types différents. La première étape consiste à effectuer l'enrôlement pour chacun de ces n SS. Les sketches $s(\text{mod}_1), \dots, s(\text{mod}_n)$
25 sont alors connus et peuvent être utilisés.

Etape n°2 :

A partir des $n-1$ premières modalités, du sketch $s(\text{mod}_n)$ et du schéma de partage de secret de Shamir, on déduit la valeur de clé.

Détail du partage de secret adapté pour fonctionner avec la présente
30 invention :

- Choisir une fonction de hachage h . On prendra par exemple $h = \text{SHA-256}$,
- Le secret est $S=s(\text{mod}_n)$. On souhaite que le seuil du partage de secret soit k avec k compris entre 2 et $n-1$,
- 5 - Choisir alors aléatoirement un polynôme $f(x) = S + a_1x + \dots + a_{k-1}x^{k-1}$.
- Pour chaque modalité, c'est-à-dire pour $i=1, \dots, n-1$, associer le couple $(h(w_i), f(h(w_i)))$ où $w_i = w(\text{mod}_i)$,
- Calculer pour $i=1$ à $n-1$, $V_i = h'(w_i)$ où h' est une fonction de hachage,
- 10 - Dans clé, stocker $f(h(w_1)), \dots, f(h(w_{n-1}))$ et $V_1, \dots, V_{n-1}$.

Remarque : la fonction de hachage est indispensable car sans elle, lorsque k « utilisateurs » (qui sont ici les modalités) retrouvent le secret S , par calculs d'antécédents il est possible de retrouver les valeurs des autres modalités. Avec la fonction de hachage, ce même calcul d'antécédents permet de ne

15 retrouver que des hachés des valeurs des autres modalités.

Phase de correction

Etape n°3 :

Le système est maintenant correctement initialisé.

Cette étape consiste à partir des $n-1$ premières modalités, à retrouver (en se

20 servant des $s(\text{mod}_i)$, $i=1, \dots, n-1$ et de clé) la valeur de $s(\text{mod}_n)$.

- Soient (au moins) k modalités valides (car il a été décidé que le seuil du partage de secret est k). Utiliser les V_i contenus dans clé pour trouver les modalités valides en comparant V_i au haché par h' de la donnée w_i trouvée. Sans perdre de généralité, nous nous
- 25 restreignons à exactement k modalités valides et supposons que ce sont les k premières modalités qui sont valides,
- A partir de clé, former les couples $(h(w_1), f(h(w_1))), \dots, (h(w_k), f(h(w_k)))$.
- En utilisant l'interpolation de Lagrange avec ces couples, retrouver
- 30 le polynôme $f(x)$ et donc son ordonnée à l'origine $S=s(\text{mod}_n)$.

A partir de la dernière modalité ainsi que de $s(\text{mod}_n)$, il est possible alors de retrouver $w(\text{mod}_n)$.

Etape n°4 :

Il faut maintenant en déduire une clé cryptographique. Pour cela
5 on applique par exemple la fonction de hachage SHA-256 sur la donnée $w(\text{mod}_n)$ pour obtenir la clé cryptographique $K : K = \text{SHA-256}(w(\text{mod}_n))$.

Lorsque $n-1$ modalités et un seuil k sont disponibles pour
l'authentification des $n-1$ premières modalités, le problème se pose de savoir
quelle sont les modalités valides. En effet, nous ne savons pas quelles
10 modalités sont valides ou non ce qui fait qu'il est possible de tomber sur un
secret ($s(\text{mod}_n)$) erroné alors que nous avons bien k modalités valides. Ce
cas se produit si l'on prend au moins une modalité non valide dans les k qui
servent à retrouver le secret grâce au schéma de partage de secret.

Deux solutions sont possibles représentées par les lettres A et B sur la figure
15 9:

- La première (lettre A) et la plus facile à mettre en œuvre est de vérifier
pour chaque modalité si elle est valide ou non. Pour cela on stocke un
haché V_i de chacun des $w(\text{mod } i)$ pour i allant de 1 à $n-1$ et on vérifie
si les modalités sont valides. Si au moins k d'entre-elles le sont, alors
20 on effectue le recouvrement du secret avec celles-ci. Sinon, il n'est
pas nécessaire de tenter de retrouver le secret (ce n'est pas possible).
- La seconde solution (lettre B) est plus difficile à mettre en œuvre mais
pourrait dans certains cas être utile. On commence par stocker un
haché V de $s(\text{mod}_n)$. Le principe est de prendre k modalités et
25 d'essayer de retrouver le secret avec. On vérifie ensuite si ce secret
est valide. On essaye cela pour les C_n^k (coefficient binomial choix de k
parmi n) choix possibles pour les k modalités. Si après avoir essayé
toutes les possibilités le secret n'est pas retrouvé, cela signifie qu'il y a
strictement moins de k modalités qui sont valides.

30 La figure 10 décrit un exemple de système permettant la mise
en œuvre du procédé selon l'invention. Le système comprend un capteur

601 relié au dispositif de mise en œuvre des étapes du procédé décrit précédemment, un support d'enregistrement 602 des clés et une mémoire de stockage des sketches.

Le procédé selon l'invention offre notamment les avantages
5 suivants : il résout notamment le problème de l'utilisation de formats et d'importances différents :

- Tailles ou types de données différents,
- Données primaires et secondaires (sécurité maîtrisée ou non) ;
- Codes correcteurs différents,
- 10 • Des métriques différentes (distance de Hamming, d'édition et symétrique) donc des secure sketches différents

Le procédé permet notamment :

- L'interopérabilité des différentes modalités (tailles, types, codes ou métriques utilisés différents) en entrée de la fonction de partage de
15 secret et en entrée du SS.
- La possibilité que chaque modalité soit traitée indépendamment des autres
- De baser la sécurité sur celle de la modalité la plus « robuste » ou bien de privilégier une modalité pour une autre raison.

REVENDICATIONS

- 1 – Procédé pour authentifier un ou plusieurs utilisateurs ou objets, voire conjointement un ou plusieurs objets ou utilisateurs en utilisant un principe
- 5 d'authentification multimodale,
- a) phase d'initialisation : définir les valeurs des sketches $s(\text{modi})$ pour chacune des modalités modi utilisées pour l'authentification, et déterminer la valeur de la donnée clé à utiliser pour une fonction de partage de secret,
- b) phase de correction : pour chacune des modalités Mod1 à Modn-1 , ledit
- 10 procédé comporte au moins les étapes suivantes :
- b1) une étape de mesure de modalité i , Modi (200i), ce qui correspond à $w'(\text{modi})$ (201i), puis une étape de traitement de la mesure $w'(\text{modi})$ (203i) en utilisant le sketch associé $s(\text{modi})$ (202i), on authentifie ainsi la donnée modi avec le secure sketch SSi pour obtenir la donnée
- 15 $w(\text{modi})$ 204i qui ne dépend que de modi ,
- b2) ces étapes (200i à 204i) sont exécutées pour toutes les modalités i choisies, i allant de 1 à $n-1$,
- b3) l'étape suivante consiste à retrouver la valeur de $s(\text{modn})$ (206) à partir de ladite donnée clé connue et à partir des différentes valeurs
- 20 $w(\text{modi})$ et d'une fonction f de partage de secret (205) afin de reconstruire le sketch $s(\text{modn})$ de la modalité n , puis
- b4) mesurer la valeur bruitée de la modalité n , c'est-à-dire obtenir $w'(\text{modn})$ (207), cette valeur étant ensuite traitée en utilisant le sketch $s(\text{modn})$ (206) et le secure sketch SSn afin de retrouver la valeur $w(\text{modn})$,
- 25 (209).
- b5) à partir de cette valeur $w(\text{modn})$, déterminer une clé cryptographique unimodale K , (210).

- 2 – Procédé selon la revendication 1 caractérisé en ce que la phase a)
- 30 d'initialisation comporte au moins les étapes suivantes :

- effectuer des mesures non bruitées $w(\text{mod}_i)$ (300i) et exécuter un secure sketch associé (301i) dans sa phase d'enrôlement afin d'obtenir le sketch $s(\text{mod}_i)$ (302i),
- mémoriser les $n-1$ premiers sketches $s(\text{mod}_i)$ dans une mémoire,
- 5 • pour trouver la valeur de clé, utiliser les différentes valeurs mesurées $w(\text{mod}_i)$ pour chacune des modalités, une fonction f de partage de secret et la valeur de sketch pour la modalité n : $s(\text{mod}_n)$.

3 – Procédé selon la revendication 1 caractérisé en ce que le procédé utilise
10 une fonction de partage de secret à seuil.

4 – Procédé selon l'une des revendications précédentes caractérisé en ce que lors de la phase d'initialisation, la valeur de clé est obtenue à partir des $n-1$ premières modalités, du sketch $s(\text{mod}_n)$ et du schéma de partage de secret de Shamir de la manière suivante :

- Choisir une fonction de hachage h avec $h = \text{SHA-512}$.
- Le secret étant $S=s(\text{mod}_n)$, établir un seuil du partage de secret k compris entre 2 et $n-1$,
- Choisir alors aléatoirement un polynôme $f(x) = S + a_1x + \dots + a_{k-1}x^{k-1}$
- 20 - Pour chaque modalité, c'est-à-dire pour $i=1, \dots, n-1$, associer le couple $(h(w_i), f(h(w_i)))$ où $w_i = w(\text{mod}_i)$,
- Calculer pour $i=1$ à $n-1$, $V_i = h'(w_i)$ où h' est une fonction de hachage,
- Dans clé, stocker $f(h(w_1)), \dots, f(h(w_{n-1}))$ et $V_1, \dots, V_{n-1}$.

25

5 – Procédé selon la revendication 4 caractérisé en ce que lors de la phase de correction, ledit procédé comporte au moins les étapes suivantes :
à partir des $n-1$ premières modalités, retrouver en se servant des $s(\text{mod}_i)$, $i=1, \dots, n-1$ et de la clé la valeur de $s(\text{mod}_n)$.

- Soient k modalités valides avec un seuil du partage de secret égal à k . Utiliser les V_i contenus dans clé pour trouver les modalités valides en comparant V_i au haché par h' de la donnée w_i trouvée,
- A partir de la donnée clé de la phase d'initialisation, former les couples $(h(w_1), f(h(w_1)))$, ..., $(h(w_k), f(h(w_k)))$, avec les k premières modalités valides,
- En utilisant l'interpolation de Lagrange avec ces couples, retrouver le polynôme $f(x)$ et donc son ordonnée à l'origine $S=s(\text{mod}_n)$, retrouver $w(\text{mod}_n)$ à partir de la dernière modalité ainsi que de $s(\text{mod}_n)$.

10

6 – Procédé selon l'une des revendications précédentes caractérisé en ce qu'il utilise une fonction de hachage par exemple la fonction de hachage SHA-256 sur la donnée $w(\text{mod}_n)$ pour obtenir la clé cryptographique K : $K=\text{SHA-256}(w(\text{mod}_n))$.

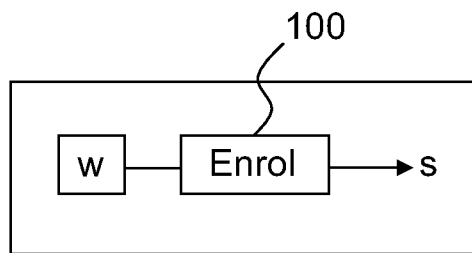
15

7 – Procédé selon la revendication 1 caractérisé en ce que la fonction de partage de secret est réalisée par une fonction « XOR » lorsque l'on utilise deux modalités et en ce que les tailles de $s(\text{mod}_2)$ et $w(\text{mod}_1)$ sont choisies identiques.

20

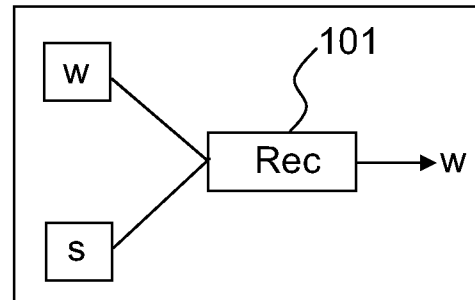
8 – Dispositif pour authentifier un ou plusieurs utilisateurs ou objets, voire conjointement un ou plusieurs objets en utilisant un principe d'authentification multimodale caractérisé en ce qu'il comporte en combinaison des moyens d'exécution (600) des étapes du procédé selon l'une des revendications 1 à 7, des moyens de mesure (601) d'une ou plusieurs modalités associées à un ou plusieurs utilisateurs et des moyens de mémorisation (602, 603).

25



Enrôlement

FIG. 1A



Recouvrement

FIG. 1B

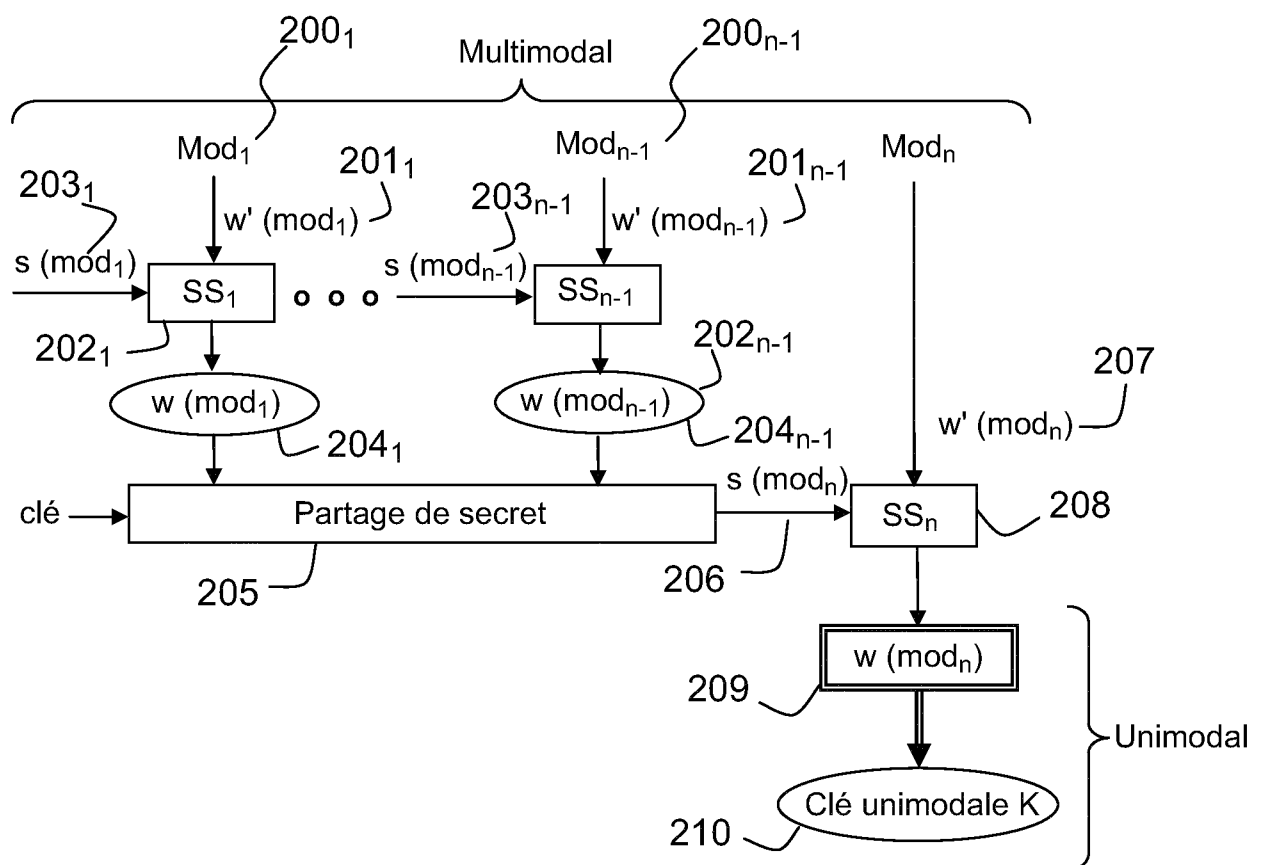


FIG. 2

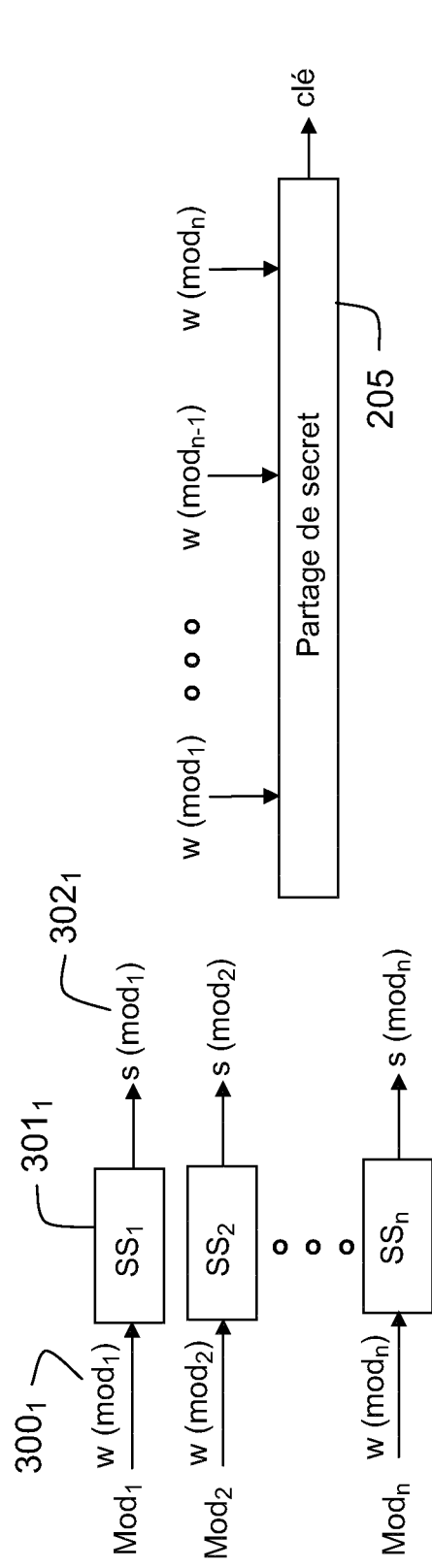
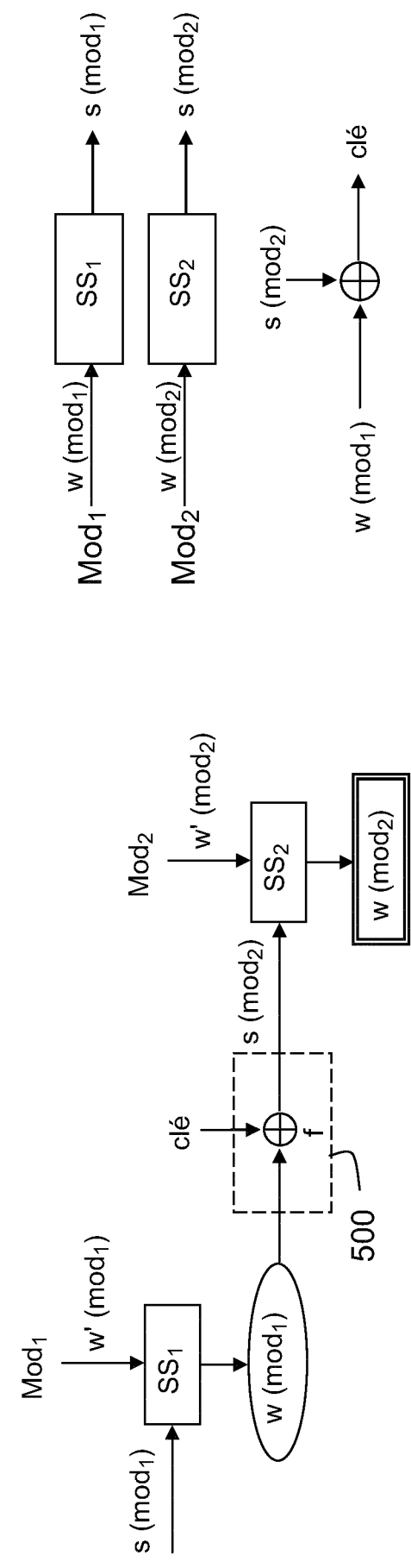
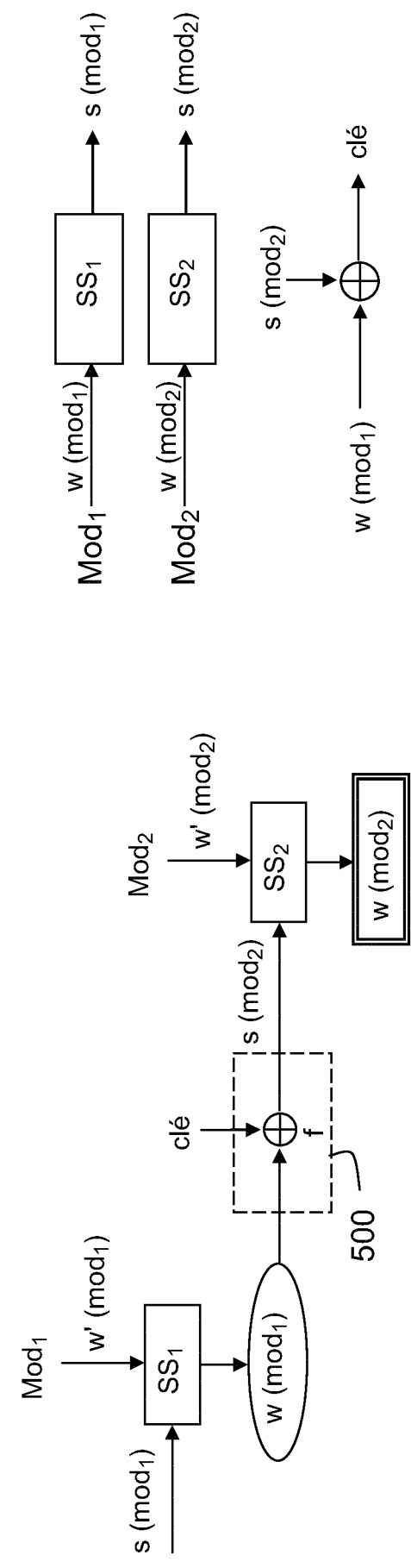
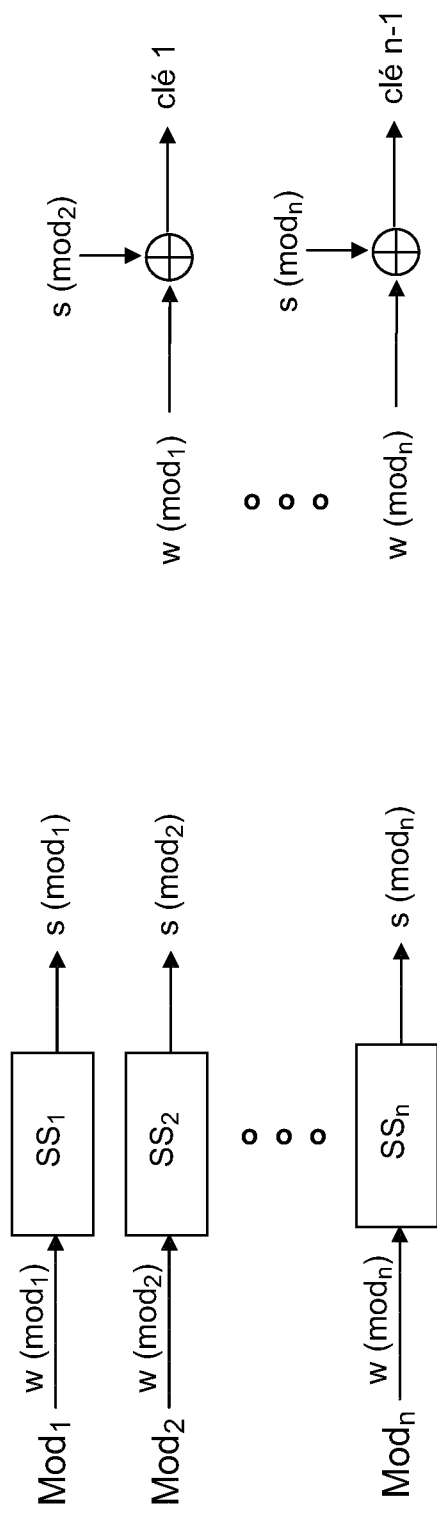
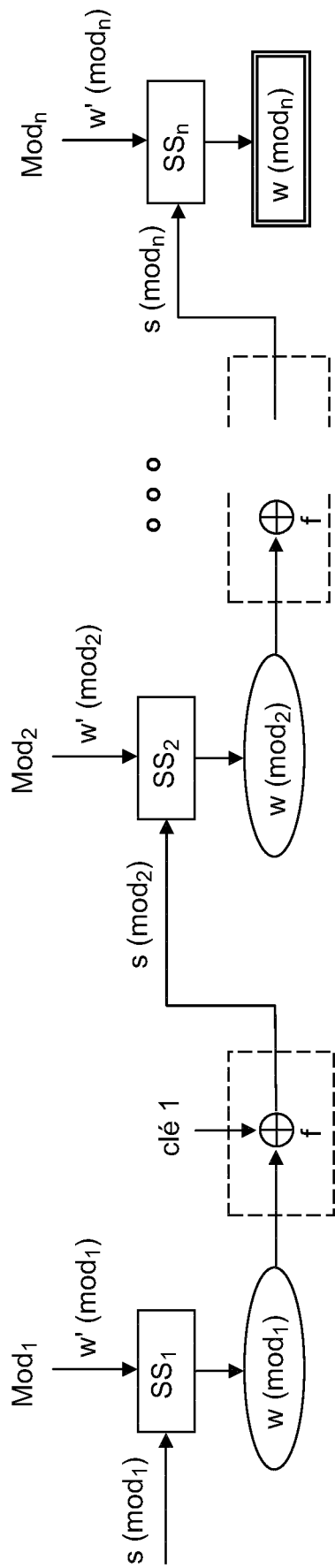
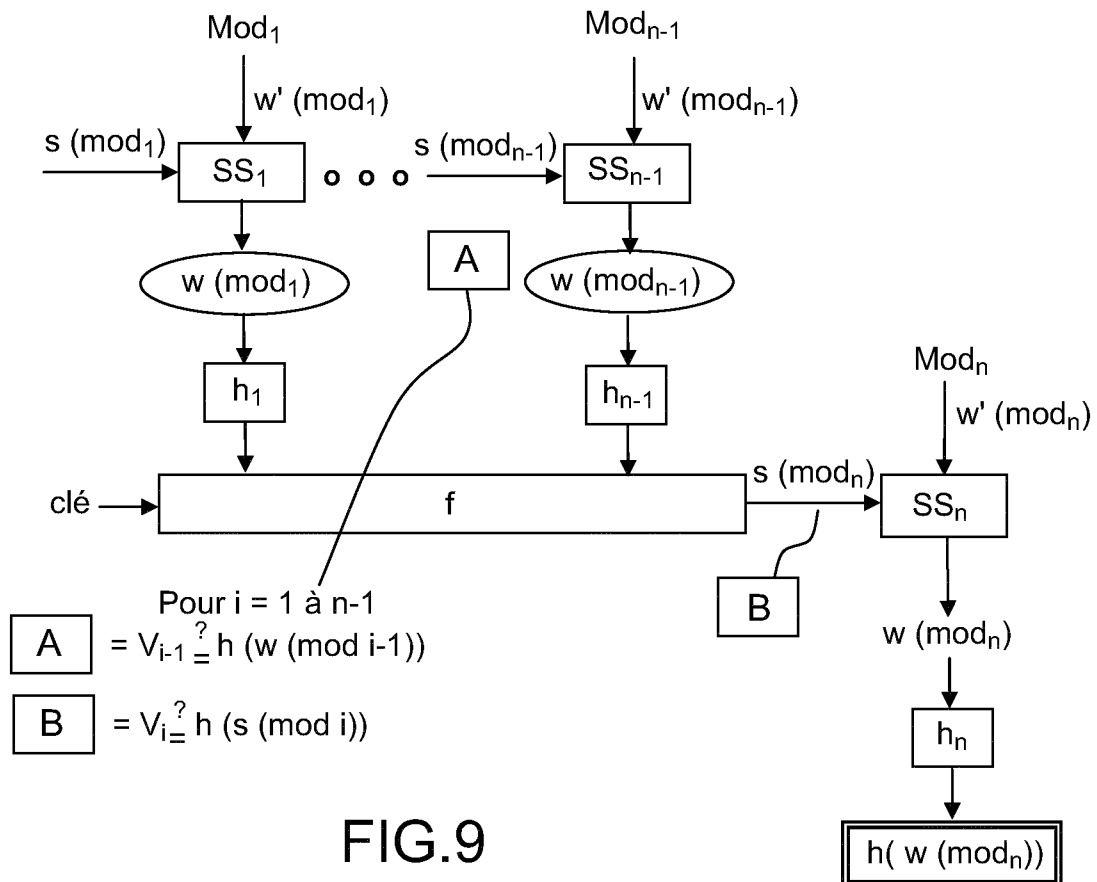
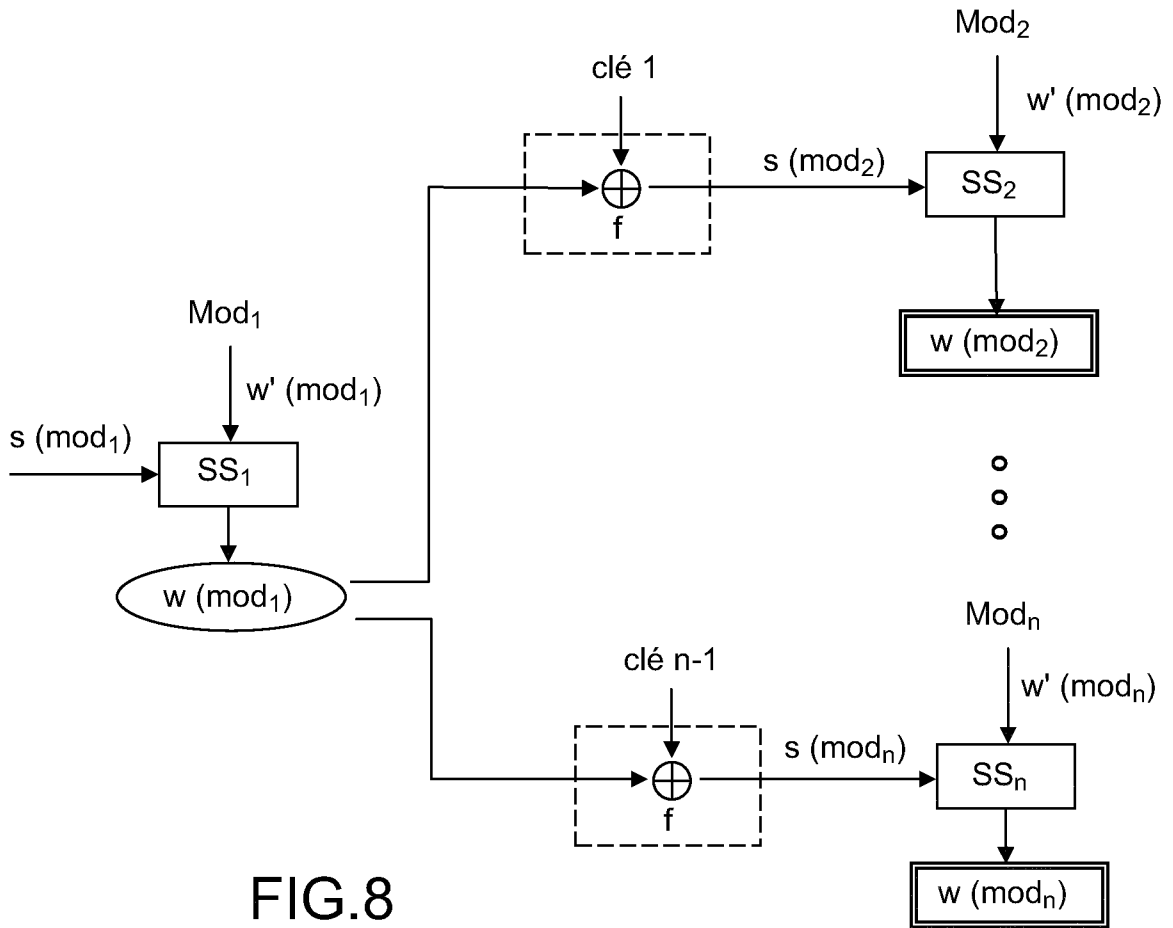


FIG.3





4/5



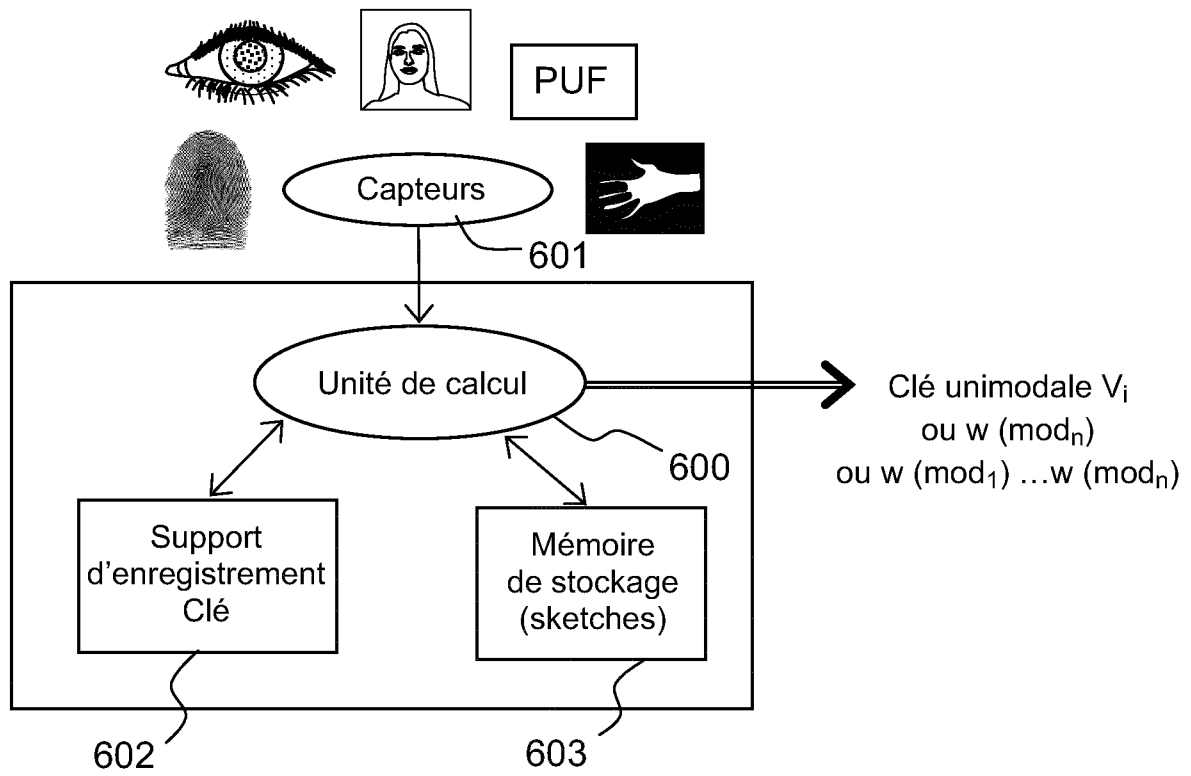


FIG.10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2011/073538

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/32
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	STELVIO CIMATO ET AL: "Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2008. ACSAC 2008. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 8 December 2008 (2008-12-08), pages 130-139, XP031376769, ISBN: 978-0-7695-3447-3 the whole document	1-8
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 - page 19, line 12 ----- -/-	1-8



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

27 January 2012

Date of mailing of the international search report

03/02/2012

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

Bec, Thierry

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2011/073538

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	VOLOSHYNOVSKIY S ET AL: "Multimodal authentication based on random projections and source coding", 20080922; 20080923 - 20080923, 22 September 2008 (2008-09-22), pages 1-10, XP007919567, paragraph [0001] - paragraph [0003] -----	1-8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2011/073538

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

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. H04L9/08 H04L9/32 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	STELVIO CIMATO ET AL: "Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System", COMPUTER SECURITY APPLICATIONS CONFERENCE, 2008. ACSAC 2008. ANNUAL, IEEE, PISCATAWAY, NJ, USA, 8 décembre 2008 (2008-12-08), pages 130-139, XP031376769, ISBN: 978-0-7695-3447-3 le document en entier	1-8
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 - page 19, ligne 12 ----- -/--	1-8
☒ 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		Date d'expédition du présent rapport de recherche internationale
27 janvier 2012		03/02/2012
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 Bec, Thierry

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	VOLOSHYNOVSKIY S ET AL: "Multimodal authentication based on random projections and source coding", 20080922; 20080923 - 20080923, 22 septembre 2008 (2008-09-22), pages 1-10, XP007919567, alinéa [0001] - alinéa [0003] -----	1-8

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2011/073538

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
