(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 925 732**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **07 60311**

(51) Int Cl[8] : ***G 06 K 9/62*** *(2006.01), G 06 F 17/15*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 21.12.07.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 26.06.09 Bulletin 09/26.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *SAGEM SECURITE Société anonyme* — FR, *CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE (CNRS)* — FR et *ECOLE NORMALE SUPERIEURE* — FR.

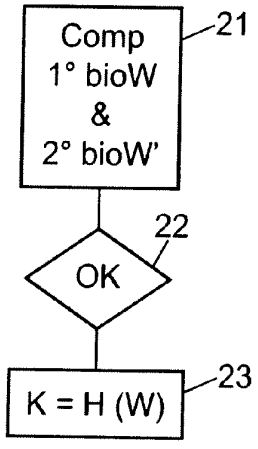
(72) **Inventeur(s) :** BRINGER JULIEN, CHABANNE HERVE, POINTCHEVAL DAVID et ZIMMER SEBASTIEN.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET PLASSERAUD.

(54) GENERATION ET UTILISATION D'UNE CLE BIOMETRIQUE.

(57) Dans un système de contrôle comprenant un dispositif de contrôle (10) adapté pour, d'une part, recevoir un signal indiquant une première donnée biométrique (w), et, d'autre part, obtenir une seconde donnée biométrique captée (w'), au niveau du dispositif de contrôle, on compare (21) les première et seconde données biométriques. Puis, on décide (22) que les première et seconde données biométriques se correspondent sur la base de la comparaison. Ensuite, on génère (23) au moins une partie de clé cryptographique secrète (H(w)) par application d'une fonction cryptographique (H) sur la première donnée biométrique.



FR 2 925 732 - A1

GENERATION ET UTILISATION D'UNE CLE BIOMETRIQUE

La présente invention concerne la génération de clés cryptographiques.

Il est important que les clés secrètes utilisées dans les systèmes cryptographiques présentent des caractéristiques permettant de conserver leur caractère secret.

A cet effet, on connait de nombreuses méthodes visant à générer de telles clés secrètes pour une utilisation cryptographique.

On peut notamment citer une méthode de génération d'aléa telle que celle décrite dans le document 'Functionality classes and evaluation methodology for physical random number generators', référencé AIS31 version 1 daté du 25/09/2001, BSI.

La présente invention vise à fournir un autre type de génération de telles clés sécrètes.

Un premier aspect de la présente invention propose un procédé de contrôle dans un système de contrôle comprenant un dispositif de contrôle adapté pour, d'une part, recevoir un signal indiquant une première donnée biométrique, et, d'autre part, obtenir une seconde donnée biométrique captée ; ledit procédé comprenant les étapes suivantes, au niveau du dispositif de contrôle :

/a/ comparer les première et seconde données biométriques ;

/b/ décider que les première et seconde données biométriques se correspondent sur la base de l'étape /a/ ; et

/c/ générer au moins une partie de clé cryptographique secrète par application d'une fonction cryptographique sur la première donnée biométrique.

Grâce à ces dispositions, il est avantageusement possible de générer une clé cryptographique offrant un niveau de protection très élevée car elle est directement issue d'une donnée biométrique d'une personne.

En outre, comme entre deux acquisitions distinctes de données biométriques captées sur une même personne il peut y avoir des différences substantielles, la connaissance de nombreuses acquisitions d'une même donnée biométrique ne permet pas de déterminer la valeur exacte de la

donnée biométrique qui est utilisée comme référence, c'est-à-dire la première donnée biométrique. Ainsi, le caractère variable de l'acquisition d'une donnée biométrique permet de garantir un niveau élevé de confidentialité de la clé obtenue selon un mode de réalisation de la présente invention. Par conséquent, la présente invention tire avantageusement partie de cette variabilité des données biométriques.

Le signal qui indique la première donnée biométrique peut provenir d'un dispositif de stockage, sur lequel est la première donnée biométrique. Ainsi, une personne munie d'un tel dispositif de stockage, sur lequel est stocké la première donnée biométrique, peut être contrôlé selon un procédé de contrôle conforme à un mode de réalisation de la présente invention. Il convient de noter que le dispositif de contrôle peut être situé au niveau du dispositif de stockage ou bien qu'il peut être situé au niveau d'un capteur servant à capter la seconde donnée biométrique.

Dans un mode de réalisation de la présente invention, c'est une clé cryptographique secrète complète qui est générée à l'étape /c/, et le système cryptographique peut en outre comprendre une base de données stockant au moins ladite clé cryptographique secrète,

ledit procédé comprenant alors en outre les étapes suivantes au niveau du dispositif de contrôle :

/d/ transmettre une requête de contrôle basée sur la clé cryptographique secrète ; et

/e/ recevoir une réponse de contrôle indiquant si la clé cryptographique secrète est stockée dans la base de données.

Ainsi, on peut aisément appliquer la clé cryptographique secrète générée selon un mode de réalisation de la présente invention, dans un contexte de contrôle d'identité d'une personne. Un tel contrôle d'identité peut correspondre soit à une authentification soit à une identification de la personne contrôlée.

Il convient de noter que dans un tel système de contrôle, la base de données peut ne contenir que des données biométriques sous forme hachée. Une telle base de données, et de ce fait un tel système de contrôle, permet d'offrir un niveau de confidentialité de données biométriques très élevé.

Par ailleurs, le contrôle est basé sur des données biométriques tout en ne mettant en œuvre que des mécanismes cryptographiques au final lors de la comparaison entre la donnée biométrique hachée reçue depuis le dispositif de contrôle et une des données biométriques stockées sous forme hachée dans la base de données.

Dans un mode de réalisation de la présente invention, on prévoit une application avantageuse de la présente invention au domaine de la signature de groupe. A cet effet, on prévoit d'associer un secret de groupe à des membres d'un groupe, chacun des membres pouvant effectuer une signature de groupe ;

ledit procédé comprenant en outre les étapes suivantes au niveau du dispositif de contrôle :

/i/ recevoir un message ;

/ii/ signer le message sur la base d'une clé cryptographique secrète comprenant, d'une part, la partie de clé cryptographique secrète générée à l'étape /c/ et, d'autre part, une autre partie de clé cryptographique secrète qui vérifie l'équation suivante :

$$A = g_1^{1/K+\gamma}$$

où K est la partie de clé cryptographique secrète générée à l'étape /c/ ;

où γ est le secret de groupe ; et

où g_1 est un paramètre public du système de contrôle ;

/iii/ transmettre, en réponse à l'étape /i/, le message signé.

Puis, en une étape ultérieure /iv/, on peut recevoir une réponse indiquant si la signature est une signature valide du groupe.

En associant un secret de groupe au groupe de signature considéré, et en prenant en compte une autre partie de clé secrète A basée à la fois sur la partie de clé secrète générée par le dispositif de contrôle et sur le secret de groupe, on peut signer un message, ou challenge qui est émis au cours d'une phase de contrôle, qui permet de prouver que celui qui a signé le message est un membre du groupe, puisque, s'il a été en mesure de signer ainsi, c'est qu'il connaît cette clé secrète complète.

Le système de contrôle peut comprendre un serveur d'enregistrement ; ledit procédé de contrôle comprenant en outre les étapes suivantes au niveau du dispositif de contrôle, avant l'étape /i/ :

- recevoir l'autre partie de clé cryptographique secrète depuis le serveur d'enregistrement ;
- stocker ladite autre partie de clé cryptographique secrète sur un dispositif de stockage.

Ainsi, dans un mode de réalisation de la présente invention, on prévoit que la personne qui souhaite signer au nom d'un groupe, soit au préalable contrôler pour décider si elle appartient à ce groupe. A cet effet, on peut prévoir, que, au cours d'une phase d'enrôlement, le dispositif de stockage de cette personne reçoive la première donnée biométrique depuis le dispositif de contrôle, permettant de générer une première partie de clé secrète, et une seconde partie de clé secrète depuis le serveur d'enregistrement. Disposant implicitement (puisque le dispositif de stockage possède la donnée biométrique permettant de générer la première partie de clé secrète) alors de la clé cryptographique complète formée des première et seconde parties de clé secrète, la personne munie de son dispositif de stockage est en mesure de prouver son appartenance au groupe de signature selon un mode de réalisation de la présente invention.

Un deuxième aspect de la présente invention propose un procédé de contrôle dans un système de contrôle comprenant un dispositif de stockage adapté pour stocker une première donnée biométrique, et un serveur d'enregistrement;

dans lequel un secret de groupe est associé à des membres d'un groupe, chacun des membres pouvant effectuer une signature de groupe ;

ledit procédé comprenant les étapes suivantes, au niveau du serveur d'enregistrement:

/a/ obtenir une première partie de clé cryptographique secrète par application d'une fonction cryptographique à la première donnée biométrique ;

/b/ générer une seconde partie de clé cryptographique secrète A selon l'équation suivante :

$A = g_1^{1/K+\gamma}$

où K est la première partie de clé cryptographique secrète ;

où γ est le secret de groupe ; et

où g_1 est un paramètre public du système de contrôle ;

/c/ transmettre la seconde partie de clé cryptographique secrète à destination du dispositif de stockage.

Ici, le serveur d'enregistrement est adapté pour générer à partir d'une première partie de clé secrète et d'un secret de groupe, une seconde partie de clé secrète, les première et seconde parties de clé secrète formant une clé cryptographique secrète adaptée pour être utilisée dans un mécanisme de signature de groupe selon un mode de réalisation de la présente invention.

Un troisième aspect de la présente invention propose un système de contrôle adapté pour mettre en œuvre un procédé de contrôle selon le premier aspect de la présente invention.

D'autres aspects, buts et avantages de l'invention apparaîtront à la lecture de la description d'un de ses modes de réalisation.

L'invention sera également mieux comprise à l'aide des dessins, sur lesquels :

- la figure 1 illustre une partie au moins d'un système de contrôle selon un mode de réalisation de la présente invention ;
- la figure 2 illustre les principales étapes d'un procédé de contrôle selon un mode de réalisation de la présente invention ;
- la figure 3 illustre un système d'identification et/ou authentification selon un mode de réalisation de la présente invention ; et
- les figures 4 et 5 illustrent un système de signature de groupe selon un mode de réalisation de la présente invention ;
- les figures 6 et 7 illustrent un système de contrôle selon deux modes de réalisation de la présente invention.

La figure 1 illustre une partie au moins d'un système cryptographique selon un mode de réalisation de la présente invention.

Un tel système comprend un dispositif de contrôle 10 adapté à la fois pour lire au moins une première donnée biométrique w qui est préalablement

stockée sur un dispositif de stockage 11 et pour capter une seconde donnée biométrique w'. Aucune limitation n'est attachée à la présente invention au regard de la localisation des différentes fonctions de stockage, de contrôle et de capture. Les figures décrites ci-dessous ne sont que pour illustrer un mode de réalisation parmi d'autres.

Ce dispositif comprend à cet effet une unité d'interface 101 pour recevoir un signal depuis le dispositif de stockage 11 lui indiquant la donnée biométrique stockée w, et un capteur 102 de données biométriques. On peut prévoir que ce capteur est en outre adapté pour déterminer si l'utilisateur est en vie et éviter des fraudes réalisées sur des personnes décédées ou virtuelles.

Aucune limitation n'est attachée au type de données biométriques qui sont manipulées dans le contexte de la présente invention. En effet, il peut s'agir par exemple, de données biométriques relatives à l'iris ou encore à une empreinte, ou tout autre.

La figure 2 illustre les principales étapes d'un procédé de contrôle selon un mode de réalisation de la présente invention, mises en œuvre au niveau du dispositif de contrôle 10.

Dans le contexte de l'invention, il est prévu d'utiliser un dispositif de stockage 11 sur lequel est stockée la première donnée biométrique w. Aucune limitation n'est attachée à la présente invention au regard du type de dispositif de stockage utilisé. On peut ainsi par exemple prévoir que ce dispositif de stockage est une clé USB (pour 'Universal Serial Bus') ou une carte à puce, ou bien encore sous la forme d'une simple impression papier (par exemple sous forme de codes barre).

Ce dispositif de contrôle 10 est alors adapté pour récupérer cette première donnée biométrique w à partir du dispositif de stockage 11. Il est également adapté pour capter une seconde donnée biométrique w'. Ainsi, lorsqu'il dispose des première et seconde données biométriques, à une étape 21, le dispositif de contrôle procède à une comparaison entre ces première et seconde données biométriques. Cette comparaison vise à déterminer si les première et seconde données biométriques sont issues d'une même personne. On peut à cette étape utiliser une des méthodes connues de comparaison

entre deux données biométriques, telle que celle décrite dans le document 'How iris recognition works ?' de J. Daugman, ou 'High Confidence Visual Recognition of Persons by a Test of Statistical Independence', 1993, IEEE Trans. on Pattern Analysis and Machine Intelligence, ou bien dans le document "Handbook of fingerprint recognition' de D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, ou bien dans le document 'Biometric Authentication: Technologies, Systems, Evaluations and Legal Issues' de J. Wayman, A. Jain, D. Maltoni and D. Maio.

Toutefois, ces exemples ne sont là qu'à titre illustratif et ne limitent en rien la réalisation de cette étape dans le contexte de la présente invention.

Ensuite, le dispositif de contrôle peut alors décider, lorsque la comparaison a permis de déterminer le fait que ces première et seconde données biométriques sont issues d'une même personne, que ces première et seconde données biométriques se correspondent, à une étape 22. Dans ce cas alors, le dispositif de contrôle 10 génère, à une étape 23, une clé cryptographique K en appliquant une fonction cryptographique H, qui peut par exemple être une fonction de hachage, à la première donnée biométrique w. L'équation suivante est vérifiée :

$$K = H(w)$$

Une telle clé cryptographique K est donc issue directement d'une donnée biométrique qui appartient à une personne. Il convient de noter que, à partir d'autres acquisitions de la même donnée biométrique, il est pratiquement impossible de retrouver la clé grâce à la variabilité importante entre les acquisitions. On peut avantageusement prévoir d'utiliser une telle clé K dans n'importe quel système cryptographique.

Ainsi, notamment, on peut prévoir de mettre en place, sur la base d'une telle clé cryptographique, un système de contrôle d'identité d'une personne, c'est-à-dire un système d'identification et/ d'authentification.

La figure 3 illustre une telle application de la présente invention dans un système de contrôle d'identité d'une personne.

Un tel système d'identification et/ou d'authentification, dans un mode de réalisation de la présente invention, comprend le dispositif de contrôle 10 ainsi

qu'une base de donnée 31 avec laquelle il est en mesure de communiquer. Cette communication entre le dispositif de contrôle 10 et la base de données 31 peut être soit une communication directe, soit une communication par l'intermédiaire d'un dispositif de gestion de base de données, qui n'est pas illustré, mais qui peut être en interface directe avec le dispositif de contrôle en recevant ses requêtes et en lui transmettant des réponses, après avoir consulté la base de données, et en interface directe avec la base de données 31 pour y consulter les données qui y son stockées.

Dans un tel système de contrôle, on peut prévoir de mettre en place une phase d'enrôlement avant toute phase de contrôle d'identité. Cette phase d'enrôlement est avantageusement effectuée de manière confidentielle.

Le contexte d'application de la présente invention ne limite en rien la mise en œuvre d'une telle phase d'enrôlement. A l'issue de cette phase d'enrôlement, la base de données 31 contient des données biométriques hachées qui correspondent respectivement aux données biométriques w stockées sur des dispositifs de stockage selon un mode de réalisation de la présente invention.

Les données biométriques hachées stockées dans la base de données sont obtenues par application d'une fonction de hachage cryptographique H aux données biométriques w stockées sur les dispositifs de stockage 11.

Puis, dans une phase de contrôle d'une personne qui dispose d'un dispositif de stockage 11 selon un mode de réalisation de la présente invention, le dispositif de contrôle 10 compare la première donnée biométrique w qui est stockée sur ce dispositif de stockage 11 avec une seconde donnée biométrique w' qu'il vient de capter sur la personne en cours de contrôle via son capteur 102.

Si le dispositif de contrôle décide que ces première et seconde données biométriques proviennent de la même personne, c'est-à-dire que la personne qui est en cours de contrôle est bien celle à qui appartient la première donnée biométrique w, alors le dispositif de contrôle 10 génère la clé cryptographique K selon un mode de réalisation de la présente invention, selon l'équation suivante :

$K = H(w)$

où H est la même fonction cryptographique, par exemple de hachage, que celle qui a été utilisée dans la phase d'enrôlement pour obtenir la forme hachée des données biométriques stockées dans la base de données 31.

Cette clé K est alors envoyée, ou plus généralement utilisée dans un protocole permettant de requérir une recherche relative à l'authentification ou l'identification, de préférence de manière sécurisée, à la base de données 31 afin de rechercher si une des données stockées dans cette base de données lui correspond. Ici, avantageusement, l'étape de recherche de correspondance entre les données biométriques hachées stockées et la donnée reçue depuis le dispositif de contrôle n'est pas entaché des problèmes liées à la biométrie et plus particulièrement au fait que deux captures de données biométriques sur une même personne peuvent être substantiellement différentes. Cette caractéristique de la biométrie complexifie beaucoup, notamment dans une base de données de grande taille, certaines comparaisons entre des données biométriques dans un contexte d'identification ou d'authentification biométrique d'une personne.

Ici, grâce aux caractéristiques décrites ci-avant, l'étape d'authentification et/ou identification correspond donc avantageusement à une étape cryptographique et non biométrique. Un tel procédé permet donc d'utiliser des données biométriques qui permettent un contrôle fournissant un niveau de sécurité élevé, tout en effectuant un contrôle d'identité dans le domaine cryptographique, et ainsi en éludant les problèmes relatifs à un tel contrôle purement biométrique.

En outre, il convient également de noter que la base de données ne contient que des données biométriques sous leur forme chiffrée de manière cryptographique, et de ce fait ne permet pas à un potentiel attaquant de récupérer des données relatives à une personne. En procédant ainsi, on préserve donc la vie privée des personnes.

Un tel système de contrôle permet d'allier le niveau de sécurité d'un contrôle biométrique aux méthodes cryptographiques de contrôle d'identité et d'authentification.

En outre, la clé K, correspondant à H(w), est facilement renouvelable, puisque deux acquisitions différentes fournissent des données biométriques distinctes, et révocable, dans le cas où une utilisation frauduleuse serait détectée.

La figure 4 illustre un système de contrôle selon un mode de réalisation de la présente invention dans une application au domaine de la signature de groupe. Dans cette application, il est prévu que la valeur K obtenue à partir de donnée biométrique d'une personne constitue une partie seulement d'une clé secrète d'un membre du groupe de signature dans le système de contrôle pour signature de groupe.

A titre illustratif, les sections suivantes décrivent une application de la présente invention au mécanisme de signature de groupe de type Boneh-Shacham tel que celui qui est décrit dans le document 'Group signatures with verifier-local revocation' de D. Boneh et H. Shacham, ACM conference on Computer and communications security, 2004.

Le système de contrôle adapté pour une méthode de signature de groupe tel qu'illustré en figure 4 comprend un dispositif de contrôle 10, un serveur de contrôle 42, un serveur d'enregistrement 44, un dispositif de gestion de clé 43 qui détient un secret γ associé aux membres d'un groupe de signature du système et un dispositif de stockage 11.

Le serveur d'enregistrement est adapté pour générer la seconde partie de clé secrète et le serveur de contrôle est adapté pour effectuer un contrôle. On peut aisément prévoir que les deux serveurs soient en fait co-localisés en un seul serveur. Une méthode de signature de groupe permet à un membre du groupe de signer un message de manière anonyme au nom du groupe et permet alors de prouver l'appartenance à un groupe.

La valeur K issue de donnée biométrique obtenue selon un mode de réalisation de la présente invention peut alors avantageusement être une partie de la clé privée utilisée au cours d'une méthode de signature de groupe.

Dans cette application, on cherche à déterminer si l'utilisateur associé à la partie K de la clé privée est un membre du groupe de signature ou non.

Il convient de noter que, avantageusement, dans un mode de réalisation de la présente invention, l'appartenance à un groupe ne requiert pas la gestion d'une base de données. Cette caractéristique est possible grâce à l'utilisation d'un secret de groupe γ associé aux membres du groupe considéré.

La figure 5 illustre un procédé de contrôle d'appartenance à un groupe de signature selon un mode de réalisation de la présente invention.

Pendant une phase d'enrôlement I, une donnée biométrique w est captée. Puis, le serveur d'enregistrement 44 en association avec le dispositif de gestion de clé 43, qui lui fournit le secret de groupe γ associé à l'utilisateur, détermine une valeur A correspondante au secret de groupe γ et à cette donnée biométrique w de telle sorte que A vérifie selon l'équation (1) suivante :

$$A^{K+\gamma} = g_1 \qquad (1)$$

où g_1 est un paramètre public du système considéré ; et

où K vérifie : K = H(w), avec H est une fonction de hachage cryptographique.

Une fois que le serveur d'enregistrement 44 a déterminé cette valeur A, il la transmet à destination du dispositif de stockage 11 dans un message 51. Cette transmission peut se faire via le dispositif de contrôle 10 qui lui, permet ensuite le stockage de la partie de clé secrète A sur le dispositif de stockage 11, comme illustré à la figure 5.

Cette valeur A est donc stockée sur le dispositif de stockage 11 de l'utilisateur. Ainsi, ce dispositif de stockage stocke la donnée (w, A) associée à l'utilisateur.

De manière alternative, on peut aussi prévoir que la donnée biométrique w est stockée dans le dispositif de stockage 11 sous une forme transformée par la fonction cryptographique. Dans ce cas, la clé cryptographique secrète complète ici est le couple (H(w), A). Par la suite, l'exemple décrit correspond à ce dernier cas.

Ainsi, dans un tel système, une clé secrète (K, A) est associée à chaque membre du groupe dans une phase d'enrôlement, où K et A vérifient les équations énoncées ci-dessus.

Dans ce contexte, l'utilisateur et son dispositif de stockage 11 contenant la clé secrète (K, A) a en charge de prouver au serveur de contrôle 42 qu'il connaît une clé vérifiant l'équation (1) afin d'être reconnu comme étant un membre du groupe.

Dans une phase de contrôle II, l'utilisateur présente son dispositif de stockage 11 au dispositif de contrôle 10.

Le dispositif de contrôle 10 capte une seconde donnée biométrique w' relative à cet utilisateur. Il tente en premier lieu de comparer les première et seconde données biométriques entre elles pour déterminer si elles sont issues de la même personne.

Dans le cas où le dispositif de contrôle décide que ces première et seconde données sont issues de la même personne, les étapes suivantes du procédé de contrôle d'appartenance à un groupe peuvent être effectuées selon un mode de réalisation de la présente invention.

La figure 5 illustre une phase d'enrôlement I et une phase de contrôle II. Au cours de la phase de contrôle, le dispositif de contrôle reçoit un message 501 indiquant un message M (ou 'challenge' en anglais) depuis le serveur de contrôle 42.

Dans le but de prouver qu'il est un membre du groupe, l'utilisateur signe le message M reçu depuis le serveur de contrôle sur la base notamment de sa clé privée (K,A).

On note :

G_1 un groupe cyclique multiplicatif d'ordre premier p ;

G_2 un groupe multiplicatif d'ordre correspondant à une puissance de p ;

Ψ est un homomorphisme depuis l'ensemble G_2 vers l'ensemble G_1 ;

G_2 est un élément d'ordre p de G_1 et g_1 est un élément générateur de G_1 de telle sorte que l'équation suivante est vérifiée :

$\Psi(g_2) = g_1$

G_T est un groupe cyclique multiplicatif d'ordre premier p ;

e est un couplage non dégénéré depuis l'ensemble $G_1 x G_2$ dans l'ensemble G_T ;

H est une fonction de hachage depuis l'ensemble {0,1}* vers Zp et H0 est une autre fonction de hachage faisant correspondre l'ensemble {0,1}* à l'ensemble G_2^2.

On note en outre gpk un groupe de clés publiques formé de la façon suivante :

$gpk = (g_1, g_2, b)$

où $b = g_2^{\gamma}$

où γ est le secret associé au groupe considéré.

La clé privée (K, A) de l'utilisateur considéré est telle que A est un élément de G_1 et K est un élément de Z_p.

K et A vérifient l'équation suivante :

$e(A, b.(g_2)^K) = e(g_1, g_2)$

K étant connu, A peut être déterminé sur la base du secret γ associé au groupe.

Le dispositif de contrôle obtient :

$(\hat{u}, \hat{v}) = H_0(gpk, M, r)$

où r est une valeur aléatoire de Z_p ;

où $\hat{u}$ u et $\hat{v}$ sont des générateurs du groupe G2

Puis, il obtient les valeurs de u et v selon les équations suivantes :

$u = \Psi(\hat{u})$; et

$v = \Psi(\hat{v})$

Ensuite, il génère une valeur aléatoire α de Z_p et calcule :

$T_1 = u^{\alpha}$;

$T_2 = A.\ v^{\alpha}$

$\delta = K\alpha$

A partir de valeurs aléatoires r_α ; r_K ; r_δ dans l'ensemble Z_p, il détermine les valeurs suivantes :

$$R_1 = u^{r_\alpha}$$

$$R_2 = e(T_2, g_2)^{r_K} . e(v, w)^{-r_\alpha} . e(v, g_2)^{-r_\delta}$$

$$R_3 = T_1^{r_K} . u^{-r_\delta}$$

On note c la valeur vérifiant l'équation suivante :

$c = H(gpk, M, r, T_1, T_2, R_1, R_2, R_3)$

Puis on calcule :

$$s_\alpha = r_\alpha + c\alpha$$

$$s_K = r_K + cK$$

$$s_\delta = r_\delta + c\delta$$

Le dispositif de contrôle est alors ensuite en mesure de transmettre au serveur de contrôle le message signé σ qui vérifie l'équation :

$\sigma = (r, c, T_1, T_2, s_\alpha, s_K, s_\delta)$

Dans un tel contexte, du côté du serveur de contrôle, on est alors en mesure de retrouver le couple de valeurs $(\hat{u}, \hat{v})$ et leur image u et v dans l'ensemble G_1.

A cet effet, le serveur de contrôle calcule :

$$\widetilde{R}_1 = u^{s_\alpha} / T_1^{c}$$

$$\widetilde{R}_2 = e(T_2, g_2)^{s_K} . e(v, w)^{-s_\alpha} . e(v, g_2)^{-s_\delta} . (e(T_2, w) / e(g_1, g_2))^{c}$$

$$\widetilde{R}_3 = T_1^{s_K} . u^{-s_\delta}$$

Ensuite il contrôle que l'équation suivante est vérifiée :

$$c = H(gpk, M, r, T_1, T_2, \widetilde{R}_1, \widetilde{R}_2, \widetilde{R}_3)$$

Si tel est le cas, le serveur de contrôle accepte la signature.

Ainsi, en utilisant la clé cryptographique K obtenue à partir d'une donnée biométrique, en tant que partie de la clé privée associé à un utilisateur d'un système de signature de groupe ; et en associant un secret de groupe γ, on est en mesure de fournir un système de signature de groupe fiable et efficace, sans gestion de base de données. Ces caractéristiques reposent sur le fait que la valeur A peut être aisément obtenue à partir de K et du secret de groupe γ.

Dans un tel contexte, une clé est facilement renouvelable, puisque deux acquisitions différentes fournissent des données biométriques distinctes, et également facilement révocable. On peut notamment prévoir de mettre un procédé de révocation comme décrit ci-après. Soit A appartenant à une liste de révocation courante, on peut prévoir alors de vérifier que l'équation suivante est vérifiée :

$$e(T_2 / A, \hat{u}) = e(T_1, \hat{v})$$

Si cette équation est vérifiée, alors on procède à la révocation.

On peut en outre prévoir de gérer la clé secrète de telle sorte qu'elle ait une durée de validité limitée, et ainsi remettre à zéro la liste de révocation régulièrement.

La figure 6 illustre un système de contrôle comprenant :

- un dispositif de stockage 11 sur lequel est stockée une première donnée biométrique w ;
- un capteur de données biométriques 102 adapté pour capter une seconde donnée biométrique ;
- un lecteur 101 de dispositif de stockage de donnée biométrique ;
- un dispositif de contrôle 10 comprenant :
  - une unité de décision 103 adaptée pour décider si les première et seconde données biométriques se correspondent sur la base d'une comparaison entre la première et la seconde donnée biométrique ; et
  - une unité de génération de clé cryptographique secrète 104 adaptée pour générer au moins une partie de clé cryptographique secrète K par application d'une fonction cryptographique H à la première donnée biométrique, lorsque l'unité de décision a décidé que les première w et seconde w' données biométriques se correspondent.

Aucune limitation n'est attachée à l'architecture relative du capteur, lecteur, du dispositif de contrôle et du dispositif de stockage.

Il convient ainsi de noter qu'il est possible que le dispositif de stockage,

le capteur et le lecteur donc, soient colocalisés.

Ou bien alternativement, on peut aussi aisément concevoir que le capteur et le lecteur sont distincts du dispositif de stockage et du dispositif de contrôle, et que le dispositif de stockage est co-localisé au dispositif de contrôle. Dans ce cas, le dispositif de stockage est un dispositif de type Match on Card (MoC).

Ce système de contrôle peut comprendre en outre :

- une base de données 31 stockant des données biométriques sous une forme transformée par la fonction cryptographique H(w).

Le dispositif de contrôle 10 comprend alors en outre une unité d'interface adaptée pour requérir auprès de la base de données un contrôle de la clé cryptographique secrète générée par l'unité de génération 104.

La figure 7 illustre un autre système de contrôle comprenant en outre un serveur de contrôle 42 adapté pour contrôler une appartenance à un groupe de membres qui peuvent effectuer une signature de groupe, un secret de groupe étant associé à ce groupe,

le dispositif de contrôle 10 comprenant en outre :

- une unité d'interface 105 avec le serveur de contrôle 42 adaptée pour recevoir 501 un message M ; et transmettre un message signé ; et
- une unité de signature 106 adaptée pour générer un message signé à partir d'un message reçu M sur la base d'une clé cryptographique secrète comprenant, d'une part, la partie de clé cryptographique secrète K générée par le dispositif de contrôle et, d'autre part, une autre partie de clé cryptographique secrète A générée par le serveur d'enregistrement 44 sur la base du secret de groupe et de ladite partie de clé cryptographique secrète.

Le serveur d'enregistrement 44 peut comprendre :

- une unité de génération 421 d'une autre partie de clé cryptographique secrète A selon l'équation suivante :

$$A = g_1^{1/K+\gamma}$$

où K est la partie de clé cryptographique secrète générée par l'unité de génération 103 du dispositif de contrôle ;

où γ est le secret de groupe ; et

où g_1 est un paramètre public du système de contrôle ;

- une unité d'interface 422 adaptée pour transmettre ladite autre partie de clé cryptographique secrète au dispositif de stockage 11.

REVENDICATIONS

1. Procédé de contrôle dans un système de contrôle comprenant un dispositif de contrôle (10) adapté pour, d'une part, recevoir un signal indiquant une première donnée biométrique (w), et, d'autre part, obtenir une seconde donnée biométrique captée (w') ;
ledit procédé comprenant les étapes suivantes, au niveau du dispositif de contrôle :

/a/ comparer (21) les première et seconde données biométriques ;

/b/ décider (22) que les première et seconde données biométriques se correspondent sur la base de l''étape /a/ ; et

/c/ générer (23) au moins une partie de clé cryptographique secrète (H(w)) par application d'une fonction cryptographique (H) sur la première donnée biométrique.

2. Procédé de contrôle selon la revendication 1, dans lequel le signal indiquant la première donnée biométrique (w) provient d'un dispositif de stockage (11), sur lequel est ladite première donnée biométrique.

3. Procédé de contrôle selon la revendication 1 ou 2, dans lequel une clé cryptographique secrète complète (K) est générée à l'étape /c/, le système cryptographique comprenant en outre une base de données (31) stockant au moins ladite clé cryptographique secrète sous une forme transformée par la fonction cryptographique ;
ledit procédé comprenant en outre les étapes suivantes au niveau du dispositif de contrôle :

/d/ transmettre une requête (32) de contrôle basée sur la clé cryptographique secrète ; et

/e/ recevoir une réponse de contrôle (33) indiquant si la clé cryptographique secrète est stockée dans la base de données.

4. Procédé de contrôle selon la revendication 1 ou 2, dans lequel un secret de groupe (γ) est associé à des membres d'un groupe, chacun des membres pouvant effectuer une signature de groupe ;

ledit procédé comprenant en outre les étapes suivantes au niveau du dispositif de contrôle (10) :

/i/ recevoir (501) un message (M) ;

/ii/ signer le message sur la base d'une clé cryptographique secrète comprenant, d'une part, la partie de clé cryptographique secrète générée à l'étape /c/ (H(w)) et, d'autre part, une autre partie de clé cryptographique secrète (A) qui vérifie l'équation suivante :

$$A = g_1^{1/K+\gamma}$$

où K est la partie de clé cryptographique secrète générée à l'étape /c/ ;

où γ est le secret de groupe ; et

où g_1 est un paramètre public du système de contrôle ;

/iii/ transmettre (52), en réponse à l'étape /i/, le message signé (σ).

5. Procédé de contrôle selon la revendication 4, dans lequel le système de contrôle comprend un serveur d'enregistrement (44),

ledit procédé de contrôle comprenant en outre les étapes suivantes au niveau du dispositif de contrôle (10), avant l'étape /i/ :

- recevoir l'autre partie de clé cryptographique secrète (A) depuis le serveur d'enregistrement ;
- stocker ladite autre partie de clé cryptographique secrète sur un dispositif de stockage (11).

6. Procédé de contrôle dans un système de contrôle comprenant un dispositif de stockage (11) adapté pour stocker une première donnée biométrique (w), et un serveur d'enregistrement (44) ;

dans lequel un secret de groupe (γ) est associé à des membres d'un groupe, chacun des membres pouvant effectuer une signature de groupe ;

ledit procédé comprenant les étapes suivantes, au niveau du serveur d'enregistrement:

/a/ obtenir une première partie de clé cryptographique secrète (K) par application d'une fonction cryptographique (H) à la première donnée biométrique (w) ;

/b/ générer une seconde partie de clé cryptographique secrète A selon l'équation suivante :

$$A = g_1^{1/K+\gamma}$$

où K est la première partie de clé cryptographique secrète ;

où γ est le secret de groupe ; et

où g_1 est un paramètre public du système de contrôle ;

/c/ transmettre la seconde partie de clé cryptographique secrète à destination du dispositif de stockage (11).

7. Système de contrôle comprenant :

- un dispositif de stockage (11) sur lequel est stockée une première donnée biométrique (w) ;
- un capteur de données biométriques (102) adapté pour capter une seconde donnée biométrique ;
- un lecteur (101) de dispositif de stockage de donnée biométrique ;
- un dispositif de contrôle (10) comprenant :
  - une unité de décision (103) adaptée pour décider si les première et seconde données biométriques se correspondent sur la base d'une comparaison entre la première et la seconde donnée biométrique ; et
  - une unité de génération de clé cryptographique secrète (104) adaptée pour générer au moins une partie de clé cryptographique secrète (K) par application d'une fonction cryptographique (H) à la première donnée biométrique, lorsque l'unité de décision a décidé que les première (w) et seconde (w') données biométriques se correspondent.

8. Système de contrôle selon la revendication 7, comprenant en outre :

- une base de données (31) stockant des données biométriques sous une forme transformée par la fonction cryptographique hachée (H(w)) ;

dans lequel le dispositif de contrôle (10) comprend en outre une unité d'interface adaptée pour requérir auprès de la base de données un contrôle de la clé cryptographique secrète générée par l'unité de génération (104).

9. Système de contrôle selon la revendication 7, comprenant en outre un serveur de contrôle (42) adapté pour contrôler une appartenance à un groupe de membres qui peuvent effectuer une signature de groupe, un secret de groupe étant associé à ce groupe,

le dispositif de contrôle (10) comprenant en outre :

- une unité d'interface (105) avec le serveur de contrôle (42) adaptée pour recevoir (501) un message (M) ; et transmettre un message signé ; et
- une unité de signature (106) adaptée pour générer un message signé à partir d'un message reçu (M) sur la base d'une clé cryptographique secrète comprenant, d'une part, la partie de clé cryptographique secrète (K) générée par le dispositif de contrôle et, d'autre part, une autre partie de clé cryptographique secrète (A) générée par le serveur d'enregistrement (42) sur la base du secret de groupe et de ladite partie de clé cryptographique secrète.

10. Système de contrôle selon la revendication 9, comprenant en outre un serveur d'enregistrement (44) qui comprend :

- une unité de génération (421) d'une autre partie de clé cryptographique secrète (A) selon l'équation suivante :

$$A = g_1^{1/K+\gamma}$$

où K est la partie de clé cryptographique secrète générée par l'unité de génération (104) du dispositif de contrôle ;

où γ est le secret de groupe ; et

où g_1 est un paramètre public du système de contrôle ;

- une unité d'interface (422) adaptée pour transmettre ladite autre partie de clé cryptographique secrète au dispositif de stockage (11).

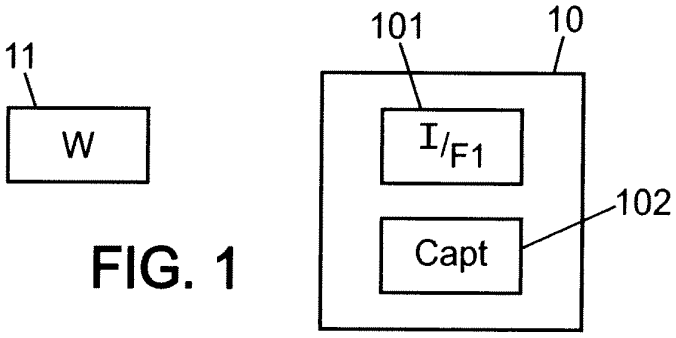


FIG. 1

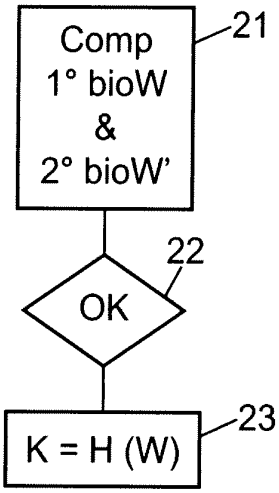


FIG. 2

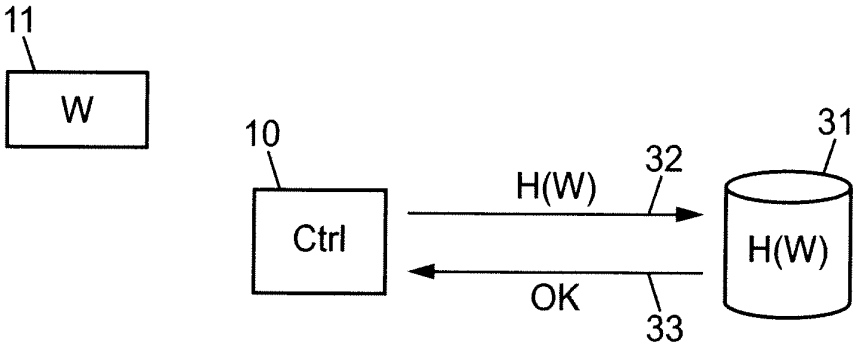


FIG. 3

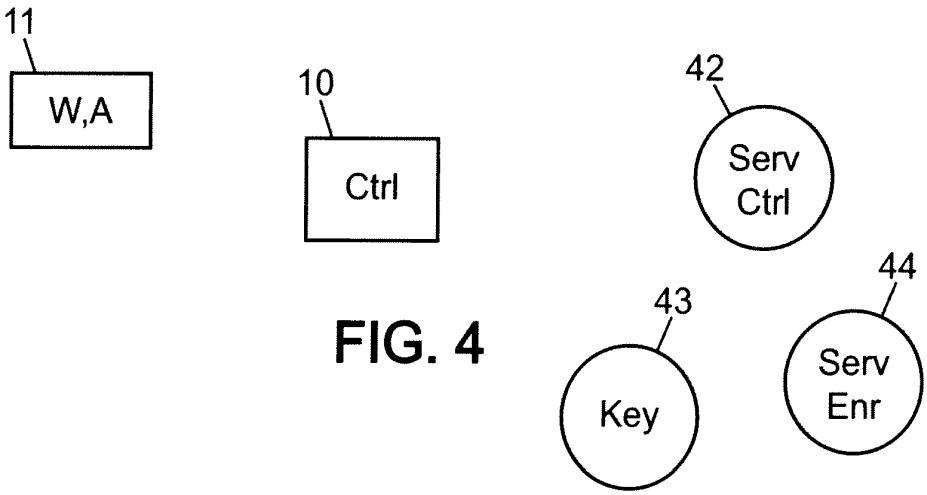


FIG. 4

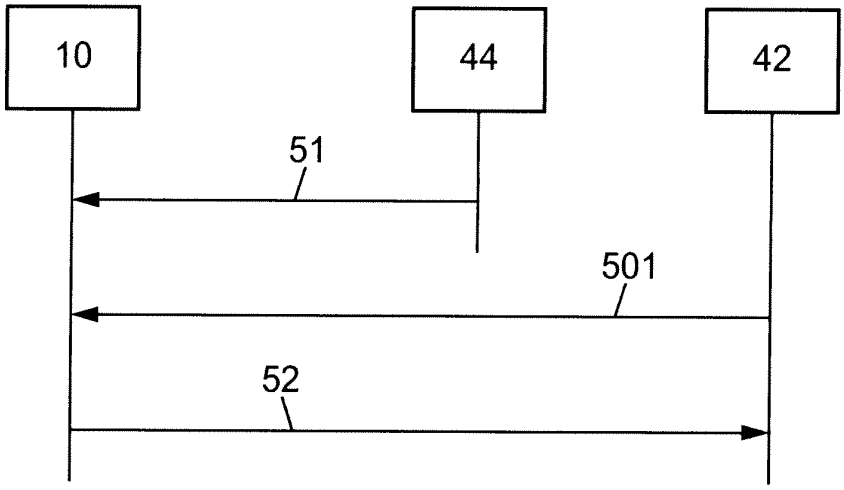


FIG. 5

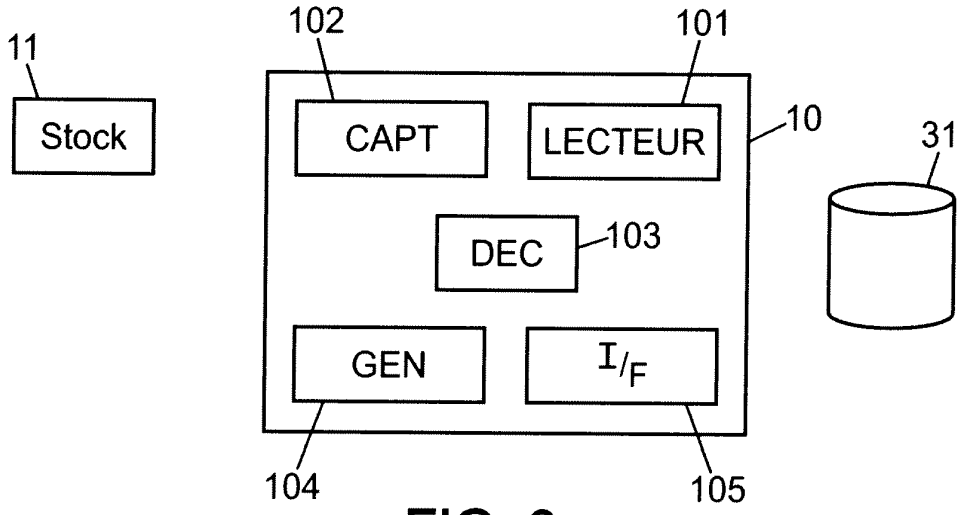

11
Stock
102
101
CAPT
LECTEUR
10
31
DEC
103
GEN
I/F
104
105

FIG. 6

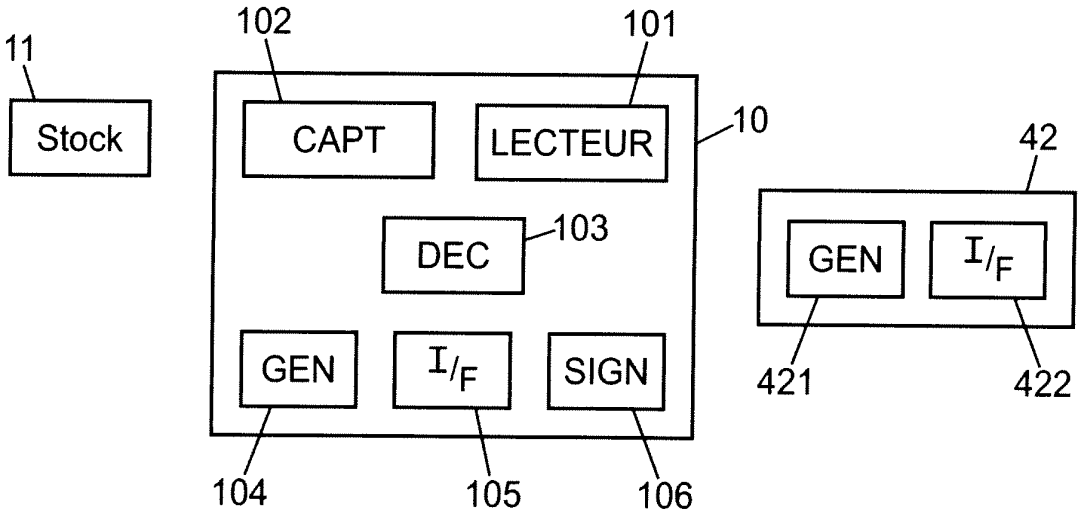

11
Stock
102
101
CAPT
LECTEUR
10
42
DEC
103
GEN
I/F
GEN
I/F
SIGN
421
422
104
105
106

FIG. 7

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 705525
FR 0760311

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	MALTONI, DAVIDE; MAIO, DARIO; JAIN, ANIL K.; PRABHAKAR, SALIL: "Handbook of Fingerprint Recognition, Chapter 9: Securing Fingerprint Systems" juin 2003 (2003-06), SPRINGER VERLAG , NEW YORK, US 280150 , XP002489873 ISBN: 0-387-95431-7	1-3,7,8	G06K9/62 G06F17/15
Y	* section 9.7, en particulier: p. 302, 2ème paragraphe, p. 305, milieu *	4-6,9,10	

D,Y	BONEH, DAN; SHACHAM, HOVAV: "Group Signatures with Verifier-Local Revocation" PROCEEDINGS OF 11TH ACM CONFERENCE ON COMMUNICATIONS AND SECURITY, CCS 04, octobre 2004 (2004-10), pages 168-177, XP007905322 Washington, DC, USA * le document en entier *	4-6,9,10	

A	JAIN A K ET AL: "Biometric Cryptosystems: Issues and Challenges" PROCEEDINGS OF THE IEEE, IEEE. NEW YORK, US, vol. 92, no. 6, 1 juin 2004 (2004-06-01), pages 948-960, XP011112757 ISSN: 0018-9219 * pages 952-953 *	1-3,7,8	DOMAINES TECHNIQUES RECHERCHÉS (IPC) G06K G06F

A	FENG HAO ET AL: "COMBINING CRYPTOGRAPHYWITH BIOMETRICS EFFECTIVELY" TECHNICAL REPORT - UNIVERSITY OF CAMBRIDGE. COMPUTER LABORATORY, XX, XX, vol. 28, no. 640, 1 juillet 2005 (2005-07-01), pages 1-17, XP009072846 * abrégé *	1-3,7,8	

	-/--		

Date d'achèvement de la recherche	Examinateur
4 août 2008	Neubüser, Bernhard

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

.....

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 705525
FR 0760311

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
A	SUJING ZHOU ET AL: "Shorter Verifier-Local Revocation Group Signatures from Bilinear Maps" CRYPTOLOGY AND NETWORK SECURITY LECTURE NOTES IN COMPUTER SCIENCE;;LNCS, SPRINGER BERLIN HEIDELBERG, BE, vol. 4301, 1 janvier 2006 (2006-01-01), pages 126-143, XP019051509 ISBN: 978-3-540-49462-1 * abrégé *	4-6,9,10	
A	XUHUA DING ET AL: "Leak-free group signatures with immediate revocation" DISTRIBUTED COMPUTING SYSTEMS, 2004. PROCEEDINGS. 24TH INTERNATIONAL C ONFERENCE ON HACHIOJI, TOKYO, JAPAN 24-26 MARCH 2004, PISCATAWAY, NJ, USA,IEEE, 24 mars 2004 (2004-03-24), pages 608-615, XP010693798 ISBN: 978-0-7695-2086-5 * abrégé *	4-6,9,10	DOMAINES TECHNIQUES RECHERCHÉS (IPC)
A	GIUSEPPE ATENIESE ET AL: "Quasi-Efficient Revocation of Group Signatures" FINANCIAL CRYPTOGRAPHY; [LECTURE NOTES IN COMPUTER SCIENCE], SPRINGER BERLIN HEIDELBERG, BERLIN, HEIDELBERG, vol. 2357, 11 mars 2002 (2002-03-11), pages 183-197, XP019053700 ISBN: 978-3-540-00646-6 * abrégé *	4-6,9,10	

Date d'achèvement de la recherche	Examinateur
4 août 2008	Neubüser, Bernhard

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

2

EPO FORM 1503 12.99 (P04C14)