(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
11 janvier 2007 (11.01.2007)

(10) Numéro de publication internationale
WO 2007/003732 A1

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

(21) Numéro de la demande internationale :
PCT/FR2006/001345

(22) Date de dépôt international : 14 juin 2006 (14.06.2006)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0506704 30 juin 2005 (30.06.2005) FR

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

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **CHABANNE, Hervé** [FR/FR]; c/o SAGEM DEFENSE SECURITE, 27, rue Leblanc, F-75015 Paris (FR).

(74) Mandataires : **ATTALI, Pascal** etc.; Cabinet Plasseraud, 52, rue de la Victoire, F-75440 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

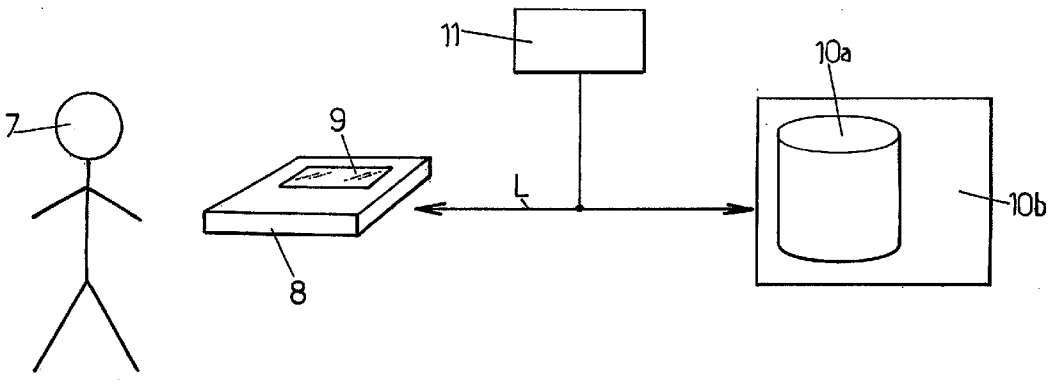
Publiée :

— *avec rapport de recherche internationale*

[Suite sur la page suivante]

(54) **Title:** METHOD FOR PROVIDING A SECURED COMMUNICATION BETWEEN A USER AND AN ENTITY

(54) **Titre :** PROCEDE POUR DISPOSER D'UN LIEN DE COMMUNICATION SECURISE ENTRE UN UTILISATEUR ET UNE ENTITE



(57) **Abstract:** The invention relates to a method for providing a secured communication between a user (1;7) and an entity (4;10b) containing a first set of biometric data (Y_0) relating to the user. According to the invention, a second set of biometric data (X_0) relating to the user is obtained. An error correction protocol is applied to the first set of biometric data and to the second set of biometric data in such a way that the resulting data is identical to a pre-determined level of probability. A secret amplification phase is implemented, in which a hashing function (G) is applied to the resulting data in order to obtain a key ($G(Y_2*),G(X_2*)$) which is common to the user and the entity.

(57) **Abrégé :** Procédé pour disposer d'un lien de communication sécurisé entre un utilisateur (1;7) et une entité (4;10b) disposant d'une première donnée biométrique (Y_0) relative à l'utilisateur. Selon le procédé, on obtient une deuxième donnée biométrique (X_0) relative à l'utilisateur. On applique un protocole de correction d'erreurs à la première donnée biométrique et à la deuxième donnée biométrique, de façon que les données résultantes soient identiques avec un niveau de probabilité prédéterminé. On met en œuvre une phase d'amplification de secret dans laquelle on applique une fonction de hachage (G) auxdites données résultantes pour obtenir une clé commune ($G(Y_2*),G(X_2*)$) à l'utilisateur et à l'entité.

WO 2007/003732 A1

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

PROCEDE POUR DISPOSER D'UN LIEN DE COMMUNICATION SECURISE ENTRE UN UTILISATEUR ET UNE ENTITE

La présente invention concerne la sécurisation d'un lien de communication entre un utilisateur et une entité.

La sécurité des communications est un enjeu majeur visant à éviter des fraudes pouvant prendre des formes diverses. En particulier, un lien de communication devrait être sécurisé de façon à empêcher un attaquant passif, à l'écoute de ce lien, de disposer de l'information qui y est transmise.

On note que le terme de lien de communication est à considérer dans un sens large. Il peut en effet s'agir d'un lien de toute nature physique, tel qu'un simple bus de communication ou un canal de télécommunication filaire ou radio, permanent ou occasionnel, et supportant tout protocole de communication.

Il a été proposé d'utiliser des données biométriques pour sécuriser un lien de communication. Les données biométriques, qui sont des informations physiques caractéristiques d'individus respectifs, telles que les empreintes digitales, l'iris des yeux, la voix, présentent en effet l'avantage d'être associées de façon naturelle et permanente à un individu.

Ainsi, il a été envisagé de calculer une clé en appliquant des algorithmes mathématiques à des données biométriques d'un utilisateur, la clé pouvant être utilisée pour sécuriser un lien de communication impliquant cet utilisateur. Dans l'esprit des initiateurs de cette technique, la clé pouvait être retrouvée à tout moment à partir d'une capture biométrique réalisée sur l'utilisateur. En outre, une telle clé devait être distinctive, c'est-à-dire différente pour chaque utilisateur. Cependant, cette technique présente des inconvénients qui la rendent difficilement réalisable en pratique.

Tout d'abord, l'acquisition d'une donnée biométrique est soumise à un aléa important. En effet, deux captures successives peuvent donner des résultats très différents, par exemple, dans le cas de captures d'empreintes digitales, en fonction de l'angle de présentation du doigt et la pression exercée par le doigt sur le capteur d'empreintes. Quelle que soit complexité des

algorithmes mathématiques mis en œuvre sur la donnée biométrique acquise, il apparaît très difficile de garantir que la clé obtenue soit toujours la même pour un utilisateur donné, tout en restant signifiante.

Par ailleurs, cette technique prend implicitement comme hypothèse que la biométrie d'un utilisateur est secrète et réservée à cet utilisateur. Cette hypothèse est erronée en réalité, puisqu'il est par exemple aisé d'obtenir les empreintes digitales d'un utilisateur par simple analyse de la surface d'objets touchés par celui-ci. Etant donné que, dans cette technique, la clé d'un utilisateur est complètement déterminée à partir de sa biométrie, un attaquant disposant de données biométriques de cet utilisateur pourrait donc obtenir sa clé et accéder ainsi librement au lien de communication impliquant cet utilisateur.

Un but de la présente invention est d'obtenir une clé de sécurité à l'aide de données biométriques, ne présentant pas les inconvénients susmentionnés.

Un autre but de l'invention est d'obtenir un lien de communication sécurisé contre les attaques passives (écoutes), à l'aide de données biométriques.

L'invention propose ainsi un procédé pour disposer d'un lien de communication sécurisé entre un utilisateur et une entité disposant d'une première donnée biométrique relative à l'utilisateur. Le procédé comprend les étapes suivantes :

- obtenir une deuxième donnée biométrique relative à l'utilisateur ;

- mettre en œuvre une phase de réconciliation d'information dans laquelle on applique un protocole de correction d'erreurs à la première donnée biométrique et à la deuxième donnée biométrique, de façon que les données résultantes soient identiques avec un niveau de probabilité prédéterminé ; et

- mettre en œuvre une phase d'amplification de secret dans laquelle on applique une fonction de hachage auxdites données résultantes pour obtenir une clé commune à l'utilisateur et à l'entité.

La deuxième donnée biométrique relative à l'utilisateur n'étant pas transmise sur un lien de communication, un éventuel attaquant ne peut s'en

saisir. Même si cet attaquant dispose d'une donnée biométrique relative à l'utilisateur, il est très peu probable que celle-ci soit identique à ladite deuxième donnée biométrique. Cela est dû notamment au fait que chaque acquisition d'une donnée biométrique comporte un grand nombre d'erreurs, c'est-à-dire de différences par rapport à une donnée de référence.

Les phases de réconciliation d'information et d'amplification de secret permettent de s'assurer qu'une clé commune à l'utilisateur et à l'entité est obtenue, sans que celle-ci puisse être également obtenue par l'attaquant ne disposant pas exactement de la deuxième donnée biométrique. Une telle clé peut alors permettre de sécuriser un lien de communication entre l'utilisateur et l'entité, par exemple par authentification ou par chiffrement des échanges.

Une phase de distillation d'avantage dans laquelle on traite la première donnée biométrique et la deuxième donnée biométrique, de façon à prendre l'avantage sur un éventuel attaquant passif, peut éventuellement être mise en œuvre avant la phase de réconciliation d'information.

Une étape préalable dans laquelle une information relative à l'utilisateur est transmise à l'entité peut également être envisagée. Cette étape peut permettre notamment un contrôle initial, de façon à ne calculer une clé de sécurité que pour des utilisateurs autorisés. Elle peut aussi permettre à l'entité de retrouver la première donnée biométrique relative à l'utilisateur lorsque l'entité dispose de données biométriques relatives à une pluralité d'utilisateurs.

De façon avantageuse, l'information transmise comprend une troisième donnée biométrique relative à l'utilisateur. Celle-ci devrait être différente de la deuxième donnée biométrique, pour éviter que cette dernière ne soit accessible à un attaquant. Elle peut par exemple résulter d'une nouvelle capture biométrique. Elle peut aussi être dérivée de la deuxième donnée biométrique, par exemple en en extrayant des minuties, ce qui présente l'avantage de ne pas nécessiter plusieurs captures biométriques successives. On peut ainsi disposer d'un lien de communication sécurisé entre un utilisateur autorisé et une entité, simplement à partir de données biométriques.

L'invention propose en outre un dispositif apte à communiquer avec une entité. Le dispositif comprend :

- des moyens pour obtenir une donnée biométrique relative à un utilisateur ;

- des moyens pour appliquer un protocole de correction d'erreurs à la donnée biométrique ; et

- des moyens de hachage de la donnée délivrée par les moyens pour appliquer un protocole de correction d'erreurs à la donnée biométrique, de façon à obtenir une clé.

L'invention propose également une entité apte à communiquer avec un utilisateur, l'entité disposant d'une première donnée biométrique relative audit utilisateur. L'entité comprend :

- des moyens pour appliquer un protocole de correction d'erreurs à la première donnée biométrique ; et

- des moyens de hachage de la donnée délivrée par les moyens pour appliquer un protocole de correction d'erreurs à la première donnée biométrique, de façon à obtenir une clé.

D'autres particularités et avantages de la présente invention apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence aux dessins annexés, dans lesquels :

- les figures 1-2 sont des schémas montrant des exemples de systèmes dans lesquels l'invention peut être mise en œuvre ;
- les figures 3-6 montrent des chaînes numériques simplifiées mises en œuvre dans un exemple de réalisation de l'invention ;
- la figure 7 est un schéma illustrant de façon simplifiée une opération de hachage mise en œuvre dans un exemple de réalisation de l'invention.

Les figures 1 et 2 montrent un utilisateur 1 ou 7 souhaitant bénéficier d'un lien sécurisé avec une entité 4 ou 10b.

Dans l'exemple illustré sur la figure 1, l'entité considérée est une carte à puce 4. Cette carte 4 peut être par exemple une carte de paiement ou une carte d'identification d'abonné telle qu'une carte SIM (Subscriber Identity Module) par exemple. La puce 5 de la carte 4 stocke des informations dépendant de l'application visée. Elle stocke en outre une donnée biométrique

de l'utilisateur 1 à qui la carte 4 appartient. La donnée biométrique en question peut être de tout type. De façon avantageuse, elle peut être définie à partir d'une empreinte digitale, d'une caractéristique de l'iris ou de la voix de l'utilisateur 1. La puce 5 comprend en outre des capacités de calcul dont certaines opérations seront détaillées par la suite.

Par ailleurs, un dispositif 2, qui est par exemple un terminal de paiement ou un terminal de communication tel qu'un téléphone portable, peut être utilisé par l'utilisateur 1. Ce terminal est agencé pour coopérer avec la carte à puce 4. Plus précisément, le terminal 2 est capable de recevoir la carte 4 par exemple dans une fente 6 prévue à cet effet. Lorsque la carte 4 est insérée dans le terminal 2, la puce 5 est en contact avec des bornes correspondantes du terminal, ce qui constitue un lien de communication entre la carte 4 et l'utilisateur 1 via le terminal 2. De plus, terminal 2 est muni de capacités de calcul dont certaines opérations seront détaillées par la suite.

Un capteur biométrique 3 est prévu pour obtenir une donnée biométrique de l'utilisateur 1. Dans l'exemple illustré sur la figure 1, ce capteur fait partie intégrante du terminal 2. On comprend cependant que le capteur pourrait être extérieur au terminal 2, tout en étant capable de transmettre au terminal 2 les données biométriques qu'il acquiert. Il est également possible qu'une donnée biométrique de l'utilisateur 1 soit acquise d'une autre façon.

La figure 2 montre un autre exemple de système dans lequel l'entité considérée est une entité distante 10b comprenant une base de données distante 10a, et avec laquelle l'utilisateur 7 souhaite pouvoir communiquer de manière sécurisée. La base de données 10a stocke par exemple des données biométriques relatives à une pluralité d'utilisateurs. L'entité 10b comprend en outre des capacités de calcul dont certaines opérations seront détaillées par la suite. Cette entité est par exemple un système informatique, tel qu'un serveur de communication.

Par ailleurs, un dispositif 8 comprenant un capteur biométrique 9 est agencé pour communiquer avec l'entité 10b. Il est en outre muni de moyens de communication pour que l'utilisateur 7 puisse disposer d'un lien de communication L avec l'entité 10b. Ce lien de communication est porté par

exemple par une liaison filaire ou par une liaison radio. De plus, le dispositif 8 est muni de capacités de calcul dont certaines opérations seront détaillées par la suite.

On suppose qu'un attaquant passif est capable d'écouter les informations échangées sur le lien de communication entre l'utilisateur 1 ou 7 et l'entité 4 ou 10b. Dans l'exemple illustré sur la figure 2, cet attaquant peut par exemple disposer une sonde sur le lien de communication L, de façon à obtenir les informations transmises sur ce lien. De plus, l'attaquant peut effectuer tout type d'opérations sur les informations acquises afin de déjouer la sécurité mise en œuvre entre l'utilisateur et l'entité. A titre d'exemple, l'attaquant peut mettre en œuvre les mêmes opérations que l'utilisateur et l'entité s'il les connaît.

Selon l'invention, on cherche à obtenir une clé, sans que l'attaquant puisse l'acquérir lui-même. Cette clé pourra ensuite être utilisée pour mettre en œuvre des mécanismes de sécurité entre le l'utilisateur et l'entité.

A cet effet, on obtient une donnée biométrique de l'utilisateur considéré, du même type que la ou les données biométriques stockées au niveau de l'entité. Par exemple, la donnée biométrique peut être obtenue par acquisition d'une empreinte digitale de l'utilisateur à l'aide d'un capteur biométrique, tels que les capteurs 3 ou 9 des figures 1 et 2 respectivement.

On considère par la suite que la donnée biométrique ainsi acquise peut être décrite par une chaîne numérique, comme la chaîne numérique X_0 de l'exemple illustré sur la figure 3. Bien sûr, d'autres représentations des données biométriques pourraient également être utilisées. Dans l'exemple choisi, la chaîne numérique X_0 comporte un nombre réduit de bits, c'est-à-dire d'éléments binaires, pour faciliter la compréhension des opérations mises en œuvre. En réalité, les chaînes numériques décrivant des données biométriques peuvent être de l'ordre de la dizaine de milliers de bits par exemple.

Par ailleurs, comme cela a été indiqué plus haut, l'entité considérée, par exemple la carte à puce 4 ou l'entité 10b des figures 1 et 2 respectivement, dispose de données biométriques relatives à un ou plusieurs utilisateurs. On suppose ci-après qu'une donnée biométrique est stockée notamment pour

l'utilisateur considéré, c'est-à-dire l'utilisateur 1 ou 7 des figures 1 et 2 respectivement. Cette donnée biométrique peut également être décrite par une chaîne numérique, telle que la chaîne numérique Y_0 représentée sur la figure 3.

On constate que les chaînes numériques X_0 et Y_0 présentent un certain nombre de différences 12 (quatre différences dans l'exemple illustré sur la figure 3). Cela est dû au fait, mentionné en introduction, qu'il existe une grande variabilité des mesures biométriques. En d'autres termes, si la chaîne numérique Y_0 est considérée, par convention, comme la chaîne de référence, toute nouvelle chaîne numérique X_0 issue d'une nouvelle acquisition de donnée biométrique comportera des "erreurs" par rapport à cette chaîne de référence. On note que d'autres choix de chaîne de référence sont également possibles, comme X_0 par exemple.

Bien sûr, ces erreurs ne sont pas prévisibles car elles dépendent de nombreux facteurs, comme de l'angle de présentation du doigt et de la pression exercée par le doigt sur le capteur lorsque les données biométriques comprennent des empreintes digitales par exemple. En outre, elles ne sont pas déterminables notamment par un attaquant passif, en particulier parce que la chaîne numérique X_0 n'est pas transmise vers l'entité.

Comme on l'a vu plus haut, un attaquant peut lui-même disposer d'une donnée biométrique relative à l'utilisateur considéré. Celle-ci a par exemple pu être acquise à partir des empreintes digitales laissées à la surface d'objets touchés par l'utilisateur. On comprend donc que la donnée biométrique ainsi obtenue par l'attaquant sera généralement moins précise que celle acquise auprès de l'utilisateur à l'aide d'un capteur biométrique par exemple. Toutefois, on peut également imaginer que l'attaquant dispose d'une donnée biométrique de l'utilisateur très fiable.

Dans l'exemple illustré sur la figure 3, on note Z_0 la chaîne numérique représentant la donnée biométrique relative à l'utilisateur, dont dispose l'attaquant. Cette chaîne numérique présente cinq erreurs, par rapport à la chaîne de référence Y_0, c'est-à-dire une erreur de plus que la chaîne numérique X_0. Dans l'exemple de la figure 3, on a choisi arbitrairement quatre

des erreurs 13 identiques aux erreurs 12. Cependant, de façon générale, on note que les erreurs contenues dans Z_0 devraient être indépendantes de celles contenues dans X_0, ces dernières étant inaccessibles à l'attaquant.

De façon avantageuse, on effectue une phase de distillation d'avantage dans laquelle on augmente la probabilité que l'attaquant ait une chaîne numérique présentant un plus grand nombre d'erreurs que la chaîne numérique obtenue côté utilisateur, par exemple par le dispositif 2 ou 8 des figures 1 et 2 respectivement. Autrement dit, cette phase permet au couple utilisateur-entité de prendre l'avantage sur l'attaquant passif. Un exemple d'opérations mises en œuvre dans une telle phase de distillation d'avantage a été divulgué par Martin Gander et Ueli Maurer, dans l'article "On the secret-key rate of binary random variables, Proc. 1994 IEEE International Symposium on Information Theory (Abstracts), 1994", p. 351. Bien sûr, d'autres opérations peuvent être mises en œuvre à condition qu'elles permettent bien de prendre l'avantage sur l'attaquant passif.

On note en outre que cette phase de distillation d'avantage peut ne pas être mise en œuvre du fait, mentionné plus haut, que l'attaquant aura généralement d'emblée une chaîne numérique comportant plus d'erreurs que celle de l'utilisateur lui-même. Toutefois, lorsqu'il existe un risque que l'attaquant dispose d'une chaîne numérique avec peu d'erreurs, il est préférable de réaliser cette phase.

Dans un exemple d'une telle phase de distillation d'avantage, les chaînes numériques X_0 et Y_0 sont décomposées en groupes de N valeurs numériques, avec N entier. Dans l'exemple illustré sur les figures 3 et 4, les bits de X_0 et Y_0 sont groupés par couple (N=2). Puis, pour chaque couple ainsi identifié, on applique un "OU exclusif" (XOR) de façon à obtenir un "1" lorsque les bits du couple considéré sont différents et un "0" lorsqu'ils sont identiques.

On compare ensuite les résultats du OU exclusif sur des groupes correspondants (c'est-à-dire de même rang) de X_0 et Y_0. Pour cela, chacun de l'utilisateur (ou du dispositif qu'il utilise) et de l'entité communique à l'autre les résultats du OU exclusif qu'il a effectué.

On détermine alors de nouvelles chaînes numériques X_1 et Y_1, en

conservant par exemple les premières valeurs numériques de chaque groupe de X_0 et Y_0 respectivement pour lequel le résultat du OU exclusif est le même que pour le groupe correspondant de l'autre chaîne numérique (Y_0 ou X_0). Les autres groupes sont ignorés et ne sont pas pris en compte dans la constitution des chaînes numériques X_1 et Y_1.

Dans l'exemple illustré sur la figure 4, on constate deux différences entre des bits du OU exclusif effectué respectivement sur X_0 et Y_0 (différences 14). On notera que le OU exclusif effectué sur l'avant-dernier couple (référence 15 sur la figure 4) a le même résultat, à savoir un "1", pour X_0 et Y_0, du fait que chacun des deux bits du couple en question de X_0 diffère des bits correspondants de Y_0.

Les chaînes numériques X_1 et Y_1 résultant de cette phase de distillation d'avantage sont représentées sur la figure 5. Y_1 devient alors la nouvelle référence. On constate que X_1 et Y_1 présentent une seule différence entre elles (différence 16), contre quatre différences entre X_0 et Y_0. On comprend ainsi que la distillation d'avantage peut faire chuter rapidement le nombre de différences entre les chaînes numériques de l'utilisateur et de l'entité.

Si l'attaquant passif décide d'agir comme le font l'utilisateur (ou le dispositif qu'il utilise) et l'entité, il peut alors capter les résultats du OU exclusif échangés entre ceux-ci et en déduire une chaîne Z_1 selon les mêmes principes. Z_1 comprend alors le premier bit de chaque couple de Z_0 ayant le même rang que deux couples correspondants de X_0 et Y_0 pour lesquels le même résultat du OU exclusif a été obtenu. Comme le montre la figure 5, la chaîne numérique Z_1 obtenue dans l'exemple comprend deux différences avec Y_1 (différences 17), soit encore une différence de plus que X_1.

La phase de distillation d'avantage peut être répétée un nombre n de fois, avec n entier, jusqu'à ce que la chaîne numérique X_n ait un taux d'erreur par rapport à Y_n inférieur à un seuil choisi. Par exemple, le nombre n peut être choisi en fonction d'un taux moyen de variabilité des mesures d'acquisition des données biométriques.

Dans l'exemple illustré sur les figures, une identité entre les chaînes numériques, côté utilisateur et côté entité, est obtenue dès la deuxième passe

de la phase de distillation d'avantage. En effet, comme cela est montré sur la figure 6, les chaînes X_2 et Y_2 sont identiques.

En revanche, la chaîne Z_2 obtenue, lors de la deuxième passe, par un attaquant passif qui met en œuvre les mêmes opérations que l'utilisateur et l'entité, reste différente de la chaîne de référence Y_2.

On peut montrer que quelle que soit la technique employée par l'attaquant pour tenter de découvrir les chaînes numériques obtenues par l'utilisateur et l'entité, cet attaquant obtiendra toujours une chaîne numérique erronée, c'est-à-dire différente de celles de l'utilisateur et de l'entité.

Une phase de réconciliation d'information est ensuite mise en œuvre. Elle consiste à éliminer encore des erreurs résiduelles dans la chaîne numérique de l'utilisateur (ou de l'entité lorsque la référence est la chaîne de l'utilisateur), pour les cas où la distillation d'avantage n'aurait pas déjà supprimé toutes les erreurs.

Dans cette phase de réconciliation d'information, un protocole de correction d'erreur est utilisé. Ce protocole devrait de préférence être choisi pour minimiser les informations transmises entre l'utilisateur et l'entité et qui pourraient représenter des informations pertinentes exploitables par l'attaquant.

Un exemple de protocole est le protocole "Cascade" décrit par de G. Brassard et L. Salvail dans l'article "Secret-key reconciliation by public discussion, EUROCRYPT '93 : Workshop on the theory and application of cryptographic techniques on Advances in cryptology, Springer-Verlag New York, Inc., 1994, pp.410-423".

Avec le protocole Cascade, les deux parties à la communication s'accordent aléatoirement et publiquement sur une permutation qu'ils appliquent respectivement sur les chaînes numériques qu'ils ont obtenues à l'issue de la distillation d'avantage. Le résultat de ces permutations est ensuite scindé en blocs de taille adaptative déterminée. Pour chaque bloc ainsi obtenu, on exécute une primitive DICHOT. Lorsque la parité des blocs correspondants pour les deux parties est identique, la primitive calculée retourne la position d'une différence au sein de ces blocs. Puis l'une des parties corrige cette erreur. Des étapes supplémentaires dites de "bactracking" sont également

prévues pour s'assurer que l'ensemble référençant tous les blocs dont la parité a été modifiée suite à la correction d'une erreur soit finalement vide.

A l'issue de la phase de réconciliation d'information, l'utilisateur et l'entité disposent d'une même chaîne numérique avec un niveau de probabilité prédéterminé. Dans l'exemple décrit en référence aux figures, on note X_2^* et Y_2^* les chaînes numériques identiques ainsi obtenues côté utilisateur et côté entité respectivement, c'est-à-dire les chaînes X_2 et Y_2 après correction. L'attaquant possède, quant à lui, une chaîne numérique Z_2^* qui diffère de X_2^* et Y_2^*, grâce notamment aux propriétés des phases de distillation d'avantage et/ou de réconciliation d'information.

Une troisième phase dite d'amplification de secret est ensuite mise en œuvre. L'objet d'une telle phase a été divulgué par Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli M. Maurer, dans l'article "Generalized privacy amplification, IEEE Transaction on Information Theory (1995)". Elle consiste à appliquer une fonction de hachage aux chaînes numériques obtenues par l'utilisateur et l'entité à l'issue de la phase précédente, c'est-à-dire à X_2^* et Y_2^* dans notre exemple.

Une fonction de hachage est une fonction de compression permettant d'obtenir une information plus courte qu'une information initiale à laquelle elle est appliquée.

Un exemple de fonction de hachage pouvant être utilisée est celui divulgué par Kaan Yüksel, dans le document "Universal hashing for ultra-low-power cryptographic hardware applications, Master's thesis, Worcester Polytechnic Institute, 2004". Cette fonction a pour avantage de requérir très peu de ressources calculatoires.

La figure 7 montre l'application de la fonction de hachage G à X_2^* et Y_2^*. Puisque $X_2^*=Y_2^*$, on a aussi $G(X_2^*)=G(Y_2^*)$. Ainsi, l'utilisateur (ou le dispositif qu'il utilise) et l'entité disposent finalement d'une même chaîne numérique de taille limitée. Dans un cas réel, $G(X_2^*)$ et $G(Y_2^*)$ sont par exemple des chaînes numériques comprenant de l'ordre d'une centaine de bits.

A l'inverse, l'attaquant dispose d'une chaîne Z_2^* différente de X_2^* et Y_2^*. Même si cet attaquant connaît la fonction de hachage utilisée par

l'utilisateur et l'entité, et tente de calculer $G(Z_2^*)$, il obtiendra ainsi une chaîne numérique différente de $G(X_2^*)$ et $G(Y_2^*)$.

En pratique, pour s'assurer que les chaînes numériques $G(X_2^*)$ et $G(Y_2^*)$ soient suffisamment signifiantes, c'est-à-dire qu'elles prennent des valeurs suffisamment distinctives en fonction des chaînes numériques de départ X_2^* et Y_2^*, on peut définir un nombre de bits seuil, de façon que $G(X_2^*)$ et $G(Y_2^*)$ soient calculés uniquement si X_2^* et Y_2^* comprennent un nombre de bits supérieur à ce seuil. Un tel seuil peut par exemple se situer entre quelques dizaines et quelques centaines de bits.

Par la suite, la chaîne numérique $G(X_2^*)=G(Y_2^*)$ commune à l'utilisateur et à l'entité peut être utilisée pour disposer d'un lien de communication sécurisé entre eux. Cette chaîne constitue ainsi une clé secrète partagée uniquement par l'utilisateur et l'entité. Elle peut par exemple permettre d'authentifier l'utilisateur. A cet effet, une information d'authentification, tel qu'un code d'identification par exemple, peut être transmise depuis l'utilisateur vers l'entité, cette information étant chiffrée à l'aide de ladite clé. La clé peut également permettre de chiffrer toute information transmise sur le lien de communication entre l'utilisateur et l'entité. D'autres applications sont également envisageables à partir de la détermination de cette clé.

Dans ce qui précède, on a supposé que la donnée biométrique relative à l'utilisateur considéré était directement disponible au niveau de l'entité. Cela peut en effet être le cas lorsque la donnée biométrique de l'utilisateur est la seule à être stockée au niveau de l'entité. Par exemple, dans le cas illustré sur la figure 1, la carte à puce 4 appartient à l'utilisateur 1 et stocke uniquement sa donnée biométrique, si bien qu'il n'existe pas d'ambiguïté sur la donnée biométrique à sélectionner pour mettre en œuvre, au niveau de la carte à puce 4, les opérations décrites plus haut.

En revanche, lorsque plusieurs données biométriques relatives à des utilisateurs différents sont stockées dans une mémoire de l'entité, comme c'est le cas de la base de données 10a de la figure 1, il convient alors de communiquer à l'entité 10b une information relative à l'utilisateur 7 qui lui permettra de retrouver la donnée biométrique correspondante, afin de lui

appliquer les opérations décrites plus haut. L'information transmise peut être de toute nature, du moment qu'il n'existe pas d'inconvénient à la transmettre de façon non sécurisée. Il peut par exemple s'agir d'une identité de l'utilisateur en question. La base de données 10a devrait alors stocker les identités de chaque utilisateur en correspondance avec leurs données biométriques, de façon à pouvoir déterminer la donnée biométrique de l'utilisateur 7, sur réception de son identité.

Dans un mode de réalisation avantageux de l'invention, un contrôle est effectué préalablement à la mise en œuvre de certaines au moins des opérations décrites plus haut, telles que les phases de distillation d'avantage, réconciliation d'information et amplification de secret. Ce contrôle vise à éviter qu'un lien sécurisé avec l'entité puisse être ouvert pour n'importe qui.

Dans ce mode de réalisation, on considère que l'entité stocke en mémoire les données biométriques des utilisateurs autorisés, c'est-à-dire pour lesquels l'utilisation d'un lien sécurisé est autorisée. Une information relative à l'utilisateur est transmise à l'entité. Après réception par l'entité, cette information servira à vérifier qu'une donnée biométrique est stockée dans la mémoire de l'entité, afin de déterminer s'il s'agit d'un utilisateur autorisé. Les opérations décrites plus haut ne seront alors mises en œuvre que s'il s'agit d'un utilisateur autorisé.

Lorsque l'entité stocke en mémoire des données biométriques relatives à une pluralité d'utilisateurs, la même information transmise par un utilisateur peut servir à vérifier qu'il s'agit d'un utilisateur autorisé et à retrouver la donnée biométrique correspondante comme décrit plus haut. Ainsi, l'information transmise peut être de toute nature, du moment qu'il n'existe pas d'inconvénient à la transmettre de façon non sécurisée. Il peut par exemple s'agir d'une identité de l'utilisateur en question.

Dans un mode de réalisation particulièrement avantageux, l'information transmise à l'entité est une donnée biométrique de l'utilisateur. Ainsi, l'ensemble des opérations mises en œuvre par l'invention, à la fois pour le contrôle initial et pour le calcul de la clé, sont réalisées à base de données biométriques.

La donnée biométrique transmise à l'entité peut par exemple résulter d'une acquisition effectuée à l'aide d'un capteur biométrique, tel que le capteur 3 ou 9 des figures 1 et 2 respectivement. On évitera cependant de transmettre la donnée biométrique (assimilable à une chaîne numérique avec les erreurs qu'elle comporte) sur laquelle les différentes opérations décrites plus haut seront effectuées. En effet, une telle transmission en clair pourrait faire l'objet d'une écoute par l'attaquant passif, qui pourrait alors être capable de calculer la clé de la même façon que l'utilisateur et l'entité.

Ainsi, si on note X_0 la chaîne numérique relative à l'utilisateur et sur laquelle les opérations décrites plus haut sont effectuées, il est possible de transmettre à l'entité une chaîne numérique X_0', issue d'une autre acquisition biométrique. Cela ne pose pas de problème car, du fait de la variabilité des mesures effectuées par le capteur biométrique, la chaîne X_0' comporte des erreurs différentes de celles présentées par X_0. Un éventuel attaquant obtenant la chaîne X_0' ne pourrait de toute façon pas en déduire une clé identique à celle obtenue par l'utilisateur à partir de X_0.

Avantageusement, la donnée biométrique transmise à l'entité peut être dérivée de celle sur laquelle les opérations décrites plus haut sont effectuées telle que la chaîne numérique X_0 de l'exemple ci-dessus. Ce mode de fonctionnement présente l'avantage que l'utilisateur n'a pas besoin de subir deux captures biométriques successives. La donnée biométrique transmise peut par exemple se présenter sous la forme de la chaîne numérique X_0 dans laquelle des modifications ont été introduites. Dans ce cas, on veillera à ce que les modifications introduites soient suffisantes pour éviter qu'un attaquant puisse retrouver la chaîne X_0.

En variante, la donnée biométrique transmise comprend des minuties, c'est-à-dire des données extraites de la donnée biométrique sur laquelle les opérations décrites plus haut sont effectuées. Par exemple, si la donnée biométrique acquise est relative à une empreinte digitale, les minuties en question peuvent comprendre quelques distances entre des points de référence de cette empreinte digitale. De cette façon, un utilisateur peut se voir attribuer une clé à partir d'une seule capture de donnée biométrique.

On comprendra que, dans les cas où l'information transmise à l'entité comprend une donnée biométrique, celle-ci pourra être utilisée par l'entité pour vérifier si l'utilisateur considéré est autorisé ou non. A cet effet, lorsque l'entité stocke en mémoire une seule donnée biométrique, comme ce pourrait être le cas dans l'exemple illustré sur la figure 1 où la carte à puce 4 stocke dans sa puce 5 la donnée biométrique relative à son utilisateur 1, le contrôle susmentionné consiste à comparer la donnée biométrique transmise à celle stockée dans la mémoire de l'entité. Lorsque l'entité stocke en mémoire une pluralité de données biométriques, comme ce pourrait être le cas dans l'exemple illustré sur la figure 2 où l'entité 10b stocke dans sa base de données 10a les données biométriques de différents utilisateurs, le contrôle susmentionné peut consister à comparer la donnée biométrique transmise à chacune des données biométriques stockées dans la mémoire de l'entité, pour détecter une éventuelle adéquation entre elles.

Si des minuties, ou d'autres données extraites d'une donnée biométrique de base sont transmises à l'entité, cette dernière devrait alors obtenir des minuties correspondantes à partir de la donnée biométrique qu'elle stocke en mémoire, afin que les minuties puissent faire l'objet d'une comparaison.

REVENDICATIONS

1. Procédé pour disposer d'un lien de communication sécurisé entre un utilisateur (1;7) et une entité (4;10b) disposant d'une première donnée biométrique (Y_0) relative à l'utilisateur, le procédé comprenant les étapes suivantes :

- obtenir une deuxième donnée biométrique (X_0) relative à l'utilisateur ;
- mettre en œuvre une phase de réconciliation d'information dans laquelle on applique un protocole de correction d'erreurs à la première donnée biométrique et à la deuxième donnée biométrique, de façon que les données résultantes soient identiques avec un niveau de probabilité prédéterminé ; et
- mettre en œuvre une phase d'amplification de secret dans laquelle on applique une fonction de hachage (G) auxdites données résultantes pour obtenir une clé commune ($G(Y_2^*),G(X_2^*)$) à l'utilisateur et à l'entité.

2. Procédé selon la revendication 1, dans lequel, avant la phase de réconciliation d'information, on met en œuvre une phase de distillation d'avantage dans laquelle on traite la première donnée biométrique (Y_0) et la deuxième donnée biométrique (X_0), de façon à prendre l'avantage sur un éventuel attaquant passif.

3. Procédé selon la revendication 1 ou 2, dans lequel le protocole de correction d'erreurs est choisi de façon à laisser fuir un minimum d'information vers un éventuel attaquant passif (11).

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel la deuxième donnée biométrique (X_0) est obtenue à l'aide d'un capteur biométrique (3;9).

5. Procédé selon l'une quelconque des revendications précédentes, comprenant une étape préalable dans laquelle une information relative à l'utilisateur (1;7) est transmise à l'entité (4;10b).

6. Procédé selon la revendication 5, dans lequel l'information transmise comprend une troisième donnée biométrique relative à l'utilisateur, dans lequel on compare les première et troisième données biométriques, les phases de réconciliation d'information et d'amplification de secret étant mises en œuvre uniquement lorsque ladite comparaison révèle une adéquation entre les première et troisième données biométriques.

7. Procédé selon la revendication 5, dans lequel l'entité (10b) dispose de données biométriques relatives à une pluralité d'utilisateurs, et dans lequel on retrouve, à l'entité, ladite première donnée biométrique à partir de l'information transmise, les phases de réconciliation d'information et d'amplification de secret étant mises en œuvre uniquement lorsque ladite première donnée biométrique a été retrouvée à partir de ladite information transmise.

8. Procédé selon la revendication 7, dans lequel l'information transmise à l'entité comprend une identité de l'utilisateur.

9. Procédé selon la revendication 7 ou 8 dans lequel l'information transmise comprend une troisième donnée biométrique relative à l'utilisateur.

10. Procédé selon la revendication 6 ou 9, dans lequel la troisième donnée biométrique comprend une information dérivée de la deuxième donnée biométrique.

11. Procédé selon la revendication 10, dans lequel la troisième donnée biométrique comprend des minuties obtenues à partir de la deuxième donnée biométrique.

12. Procédé selon la revendication 6 ou 9, dans lequel la troisième donnée biométrique est obtenue à l'aide d'un capteur biométrique (3;9) et est distincte de la deuxième donnée biométrique.

13. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre une étape ultérieure d'authentification dans laquelle l'utilisateur transmet à l'entité une information grâce à laquelle l'entité peut

authentifier l'utilisateur, ladite information étant chiffrée à l'aide de la clé obtenue.

14. Dispositif (2;8) apte à communiquer avec une entité (4;10b), comprenant :

- des moyens pour obtenir une donnée biométrique (X_0) relative à un utilisateur (1;7) ;

- des moyens pour appliquer un protocole de correction d'erreurs à la donnée biométrique ; et

- des moyens de hachage de la donnée (X_2*) délivrée par les moyens pour appliquer un protocole de correction d'erreurs à la donnée biométrique, de façon à obtenir une clé ($G(X_2$*)).

15. Dispositif selon la revendication 14, dans lequel les moyens pour obtenir une donnée biométrique (X_0) relative à un utilisateur comprennent un capteur biométrique (3;9).

16. Dispositif selon la revendication 14 ou 15, comprenant en outre des moyens pour mettre en œuvre une phase de distillation d'avantage dans laquelle on traite la donnée biométrique (X_0), de façon à prendre l'avantage sur un éventuel attaquant passif (11).

17. Dispositif selon l'une quelconque des revendications 14 à 16, comprenant en outre des moyens pour transmettre à l'entité (4;10b) une information relative à l'utilisateur (1;7).

18. Dispositif selon l'une quelconque des revendications 14 à 17, comprenant en outre des moyens pour transmettre à l'entité (4;10b) une information d'authentification chiffrée à l'aide de la clé obtenue.

19. Entité (4;10b) apte à communiquer avec un utilisateur (1;7), l'entité disposant d'une première donnée biométrique (Y_0) relative audit utilisateur, l'entité comprenant :

- des moyens pour appliquer un protocole de correction d'erreurs à la première donnée biométrique ; et

- des moyens de hachage de la donnée (Y_2*) délivrée par les moyens pour appliquer un protocole de correction d'erreurs à la première donnée biométrique, de façon à obtenir une clé ($G(Y_2*)$).

20. Entité selon la revendication 19, comprenant en outre des moyens pour mettre en œuvre une phase de distillation d'avantage dans laquelle on traite la première donnée biométrique (Y_0), de façon à prendre l'avantage sur un éventuel attaquant passif.

21. Entité selon la revendication 19 ou 20, comprenant en outre des moyens pour recevoir une information relative à l'utilisateur (1;7).

22. Entité selon la revendication 21, dans laquelle ladite information relative à l'utilisateur comprend une seconde donnée biométrique relative à l'utilisateur (1;7), l'entité comprenant en outre des moyens de comparaison entre les première et seconde données biométriques, les moyens pour appliquer un protocole de correction d'erreurs à la première donnée biométrique et les moyens de hachage étant mis en œuvre uniquement lorsque lesdits moyens de comparaison révèlent une adéquation entre les première et seconde données biométriques.

23. Entité selon la revendication 21, l'entité disposant de données biométriques relatives à une pluralité d'utilisateurs et comprenant en outre des moyens pour retrouver ladite première donnée biométrique à partir de ladite information relative à l'utilisateur (1;7), les moyens pour appliquer un protocole de correction d'erreurs à la première donnée biométrique et les moyens de hachage étant mis en œuvre uniquement lorsque ladite première donnée biométrique a été retrouvée à partir de ladite information relative à l'utilisateur.

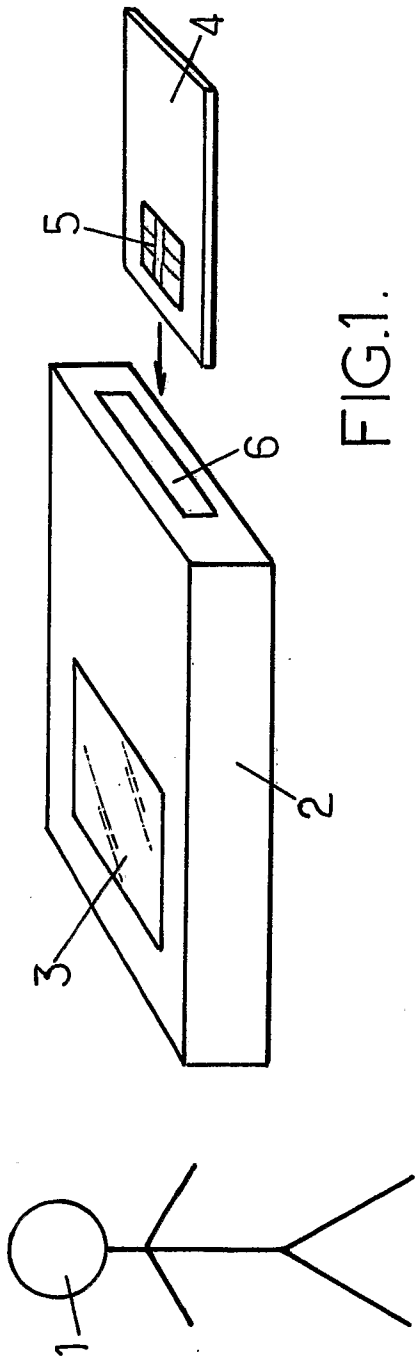


FIG.1.

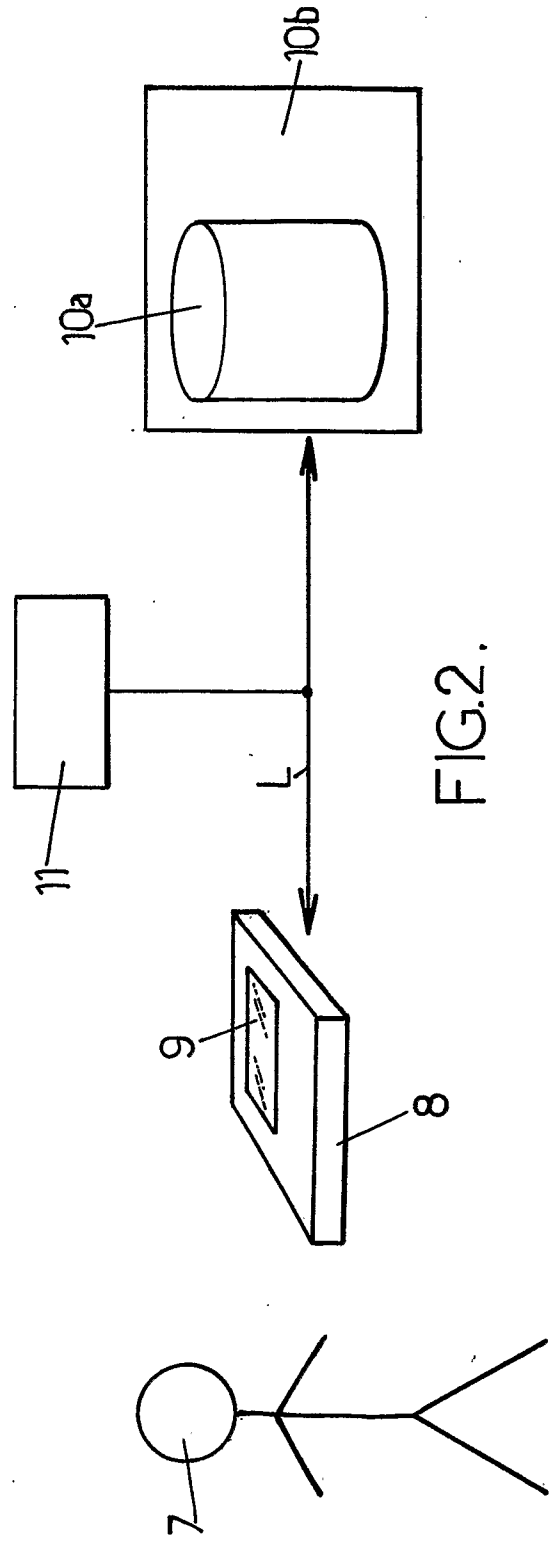


FIG.2.

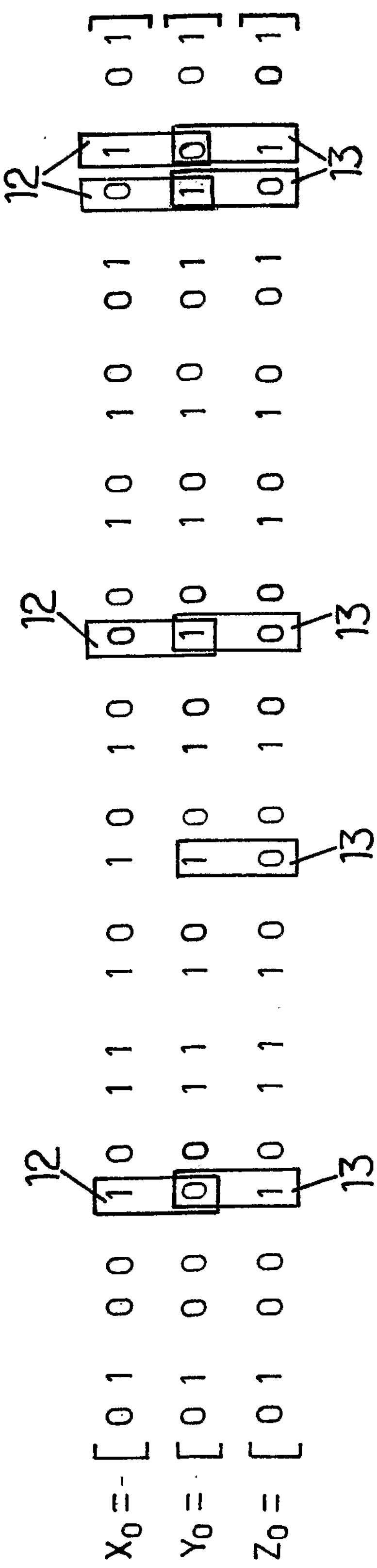


FIG.3.

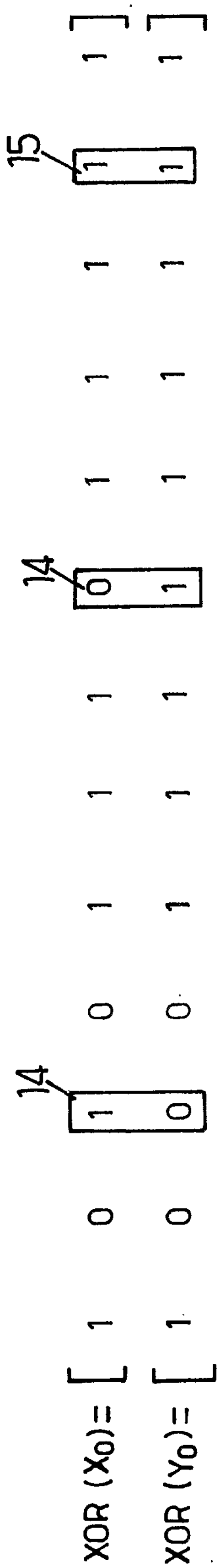


FIG.4.

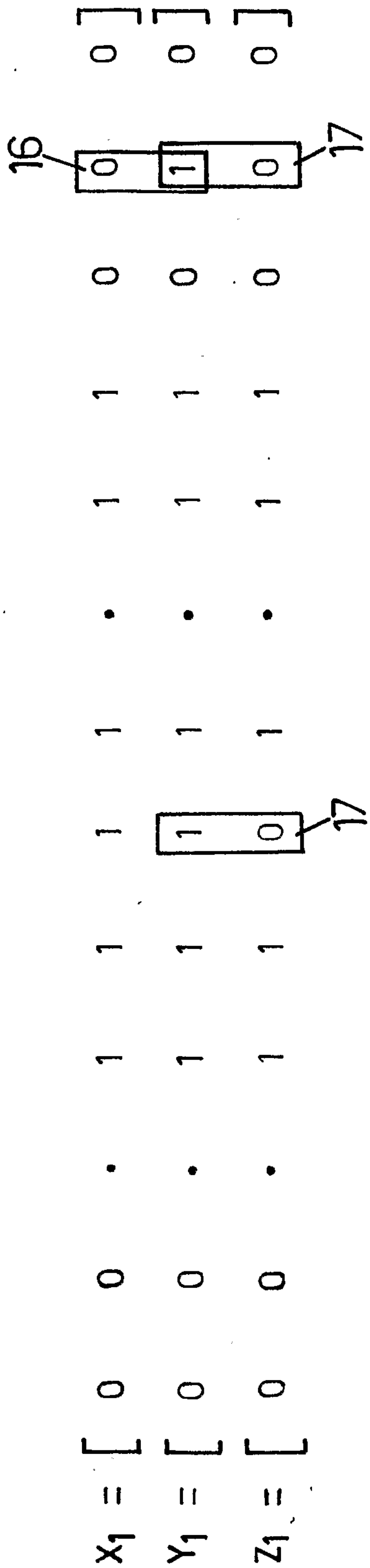


FIG.5.

$$x_2 = [0\ 1\ 1\ 1]$$
$$y_2 = [0\ 1\ 1\ 1]$$
$$z_2 = [0\ 1\ 0\ 1]$$

FIG.6.

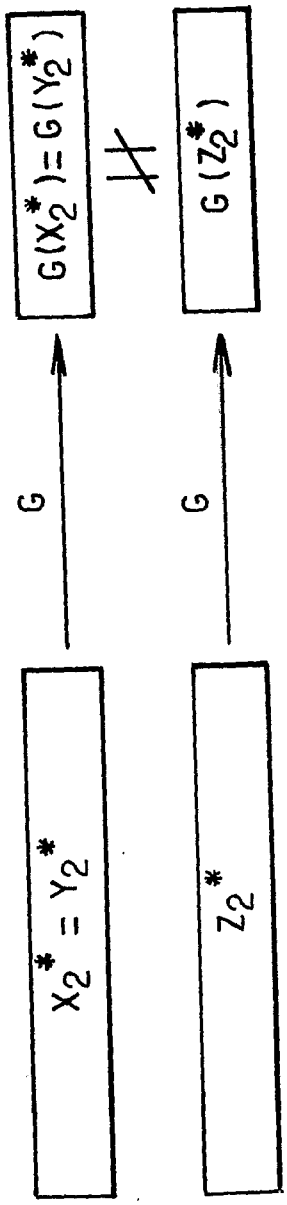


FIG.7.

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/001345

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08

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, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 363 485 B1 (ADAMS CARLISLE ET AL) 26 March 2002 (2002-03-26) abstract column 2, line 31 - column 6, line 3; figures 2-6	1,4,5,7, 8,14,15, 17-19, 21,23
X	WO 00/51244 A (RSA SECURITY INC; JUELS, ARI; WATTENBERG, MARTIN, M) 31 August 2000 (2000-08-31) abstract page 8, line 12 - page 27, line 17; figures 1,6-19	1,4,5, 13-15, 17-19,21

-/--

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

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 October 2006	20/10/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dujardin, Corinne

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2006/001345

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	LIU S ET AL: "A practical protocol for advantage distillation and information reconciliation" DESIGNS, CODES AND CRYPTOGRAPHY, KLUWER ACADEMIC PUBLISHERS, BOSTON, US, 2003, pages 39-62, XP002337939 ISSN: 0925-1022 the whole document	1-3,14, 16,19,20
X	BENNETT C H ET AL: "GENERALIZED PRIVACY AMPLIFICATION" IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 41, no. 6, PART 2, November 1995 (1995-11), pages 1915-1923, XP000823297 ISSN: 0018-9448 cited in the application the whole document	1,2,14, 16,19,20

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2006/001345

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6363485 B1	26-03-2002	NONE	
WO 0051244 A	31-08-2000	AT 255787 T	15-12-2003
		AU 3228600 A	14-09-2000
		CA 2362882 A1	31-08-2000
		DE 60006935 D1	15-01-2004
		DE 60006935 T2	04-11-2004
		EP 1149475 A1	31-10-2001
		JP 2002538504 A	12-11-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/001345

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

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 estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 6 363 485 B1 (ADAMS CARLISLE ET AL) 26 mars 2002 (2002-03-26) abrégé colonne 2, ligne 31 - colonne 6, ligne 3; figures 2-6	1,4,5,7, 8,14,15, 17-19, 21,23
X	WO 00/51244 A (RSA SECURITY INC; JUELS, ARI; WATTENBERG, MARTIN, M) 31 août 2000 (2000-08-31) abrégé page 8, ligne 12 - page 27, ligne 17; figures 1,6-19	1,4,5, 13-15, 17-19,21

-/--

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

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant 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'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion 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
13 octobre 2006	20/10/2006

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dujardin, Corinne

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2006/001345

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	LIU S ET AL: "A practical protocol for advantage distillation and information reconciliation" DESIGNS, CODES AND CRYPTOGRAPHY, KLUWER ACADEMIC PUBLISHERS, BOSTON, US, 2003, pages 39-62, XP002337939 ISSN: 0925-1022 le document en entier	1-3,14, 16,19,20
X	BENNETT C H ET AL: "GENERALIZED PRIVACY AMPLIFICATION" IEEE TRANSACTIONS ON INFORMATION THEORY, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 41, no. 6, PART 2, novembre 1995 (1995-11), pages 1915-1923, XP000823297 ISSN: 0018-9448 cité dans la demande le document en entier	1,2,14, 16,19,20

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2006/001345

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6363485 B1	26-03-2002	AUCUN	
WO 0051244 A	31-08-2000	AT 255787 T	15-12-2003
		AU 3228600 A	14-09-2000
		CA 2362882 A1	31-08-2000
		DE 60006935 D1	15-01-2004
		DE 60006935 T2	04-11-2004
		EP 1149475 A1	31-10-2001
		JP 2002538504 A	12-11-2002