(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 870 413**

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

(21) **N° d'enregistrement national :** **04 05236**

(51) Int Cl[7] : **H 04 L 9/32,** G 06 K 9/62

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 14.05.04.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 18.11.05 Bulletin 05/46.

(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) :** *GEMPLUS Société anonyme* — FR.

(72) **Inventeur(s) :** NACCACHE DAVID, BRIER ERIC, CARDONNEL CEDRIC et CORON JEAN SEBASTIEN.

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

(74) **Mandataire(s) :** NOVAGRAAF TECHNOLOGIES (CABINET BALLOT).

(54) PROCEDE DE CHIFFREMENT DE DONNES NUMERIQUES, PROCEDE DE MASQUAGE D'UNE EMPREINTE BIOMETRIQUE, ET APPLICATION A LA SECURISATION D'UN DOCUMENT DE SECURITE.

(57) L'invention concerne un procédé de masquage d'une donnée claire b de n bits, caractérisé en ce qu'on produit une donnée chiffrée m en utilisant la fonction de masquage suivante:

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$$

, où p est un nombre premier, b_i est le bit de rang i de la donnée claire b, q_i est le nombre premier de rang i d'un ensemble de nombres premiers $(q_1, ..., q_n)$.

L'invention concerne également un procédé de masquage d'une empreinte biométrique au cours duquel on détermine un ensemble de s minuties réelles caractéristiques de la dite empreinte, caractérisé en ce qu'ensuite, on mélange et on range les minuties réelles avec t fausses minuties puis on forme une donnée biométrique mélangée b de n = s + t bits telle que, pour tout i:

$b_i = 1$ si le rang i correspond à une minutie réelle et

$b_i = 0$ si le rang i correspond à une fausse minutie.

Application à la sécurisation d'un document de sécurité tel qu'un chèque bancaire.

FR 2 870 413 - A1

PROCEDE DE CHIFFREMENT DE DONNEES NUMERIQUE, PROCEDE DE MASQUAGE D'UNE EMPREINTE BIOMETRIQUE, ET APPLICATION A LA SECURISATION D'UN DOCUMENT DE SECURITE

L'invention a pour objet les systèmes d'identification et / ou d'authentification biométrique. Ces systèmes manipulent des données biométriques de tous types telles que par exemple des empreintes digitales, des empreintes numériques de l'œil, de la peau, du visage, ou même de la voix.

L'utilisation d'empreintes biométriques est de plus en plus envisagée pour compléter des mots de passe utilisateur ou une signature manuelle, notamment pour des applications nécessitant un haut niveau de sécurité. En effet, l'utilisation d'une empreinte biométrique est un bon complément à un mot de passe ou une signature manuelle, dans la mesure où une empreinte biométrique peut difficilement être dérobée à son propriétaire réel et ne peut pas non plus être imitée, copiée. En contrepartie de cette sécurité et dans la mesure où une empreinte biométrique ne peut pas être remplacée, il est indispensable d'empêcher l'accès direct à cette empreinte afin de garantir la sécurité des personnes et la fiabilité de l'empreinte.

Pour cela, on peut par exemple envisager des procédés de masquage connus pour masquer l'empreinte biométrique à sécuriser. L'empreinte masquée peut être ensuite utilisée en lieu et place de l'empreinte claire, pour signer un message, authentifier l'identité d'une personne, etc. L'intérêt de tels procédés est l'utilisation de fonctions de hachage, qui sont des fonctions à sens unique, c'est-à-dire qu'elles ne peuvent pas être inversées. En

d'autres termes, connaissant une empreinte masquée par une fonction de hachage à partir d'une empreinte claire, il n'est pas possible de retrouver l'empreinte claire, même en connaissant tous les paramètres de la fonction de hachage.

Il est bien connu par ailleurs qu'il n'est pas possible de prendre deux empreintes biométriques strictement identiques d'un même individu à des instants différents. D'abord parce qu'il est très difficile de positionner, de manière strictement identique mais à des instants différents, un même instrument de mesure adapté pour relever la dite empreinte biométrique. Ensuite par ce que l'environnement (température, humidité, etc.) et l'état de santé général (stress, maladie de peau, etc.) de l'individu au moment où l'empreinte est relevée peut perturber le résultat du relevé.

Or, avec les fonctions de chiffrement connues, partant de deux données initiales peu différentes, les données chiffrées correspondantes sont très différentes et décorrélées, il n'est donc pas possible, en les comparant, d'en déduire si les données initiales sont identiques à quelques erreurs près ou pas. Il n'est donc pas possible d'utiliser les fonctions de chiffrement connues pour chiffrer une empreinte biométrique.

Un premier objet de l'invention est de proposer une nouvelle fonction de masquage, mieux adaptée pour chiffrer des empreintes biométriques que les fonctions de chiffrement connues. Un deuxième objet de l'invention est un procédé de masquage bien adapté pour sécuriser une empreinte biométrique. Enfin, un troisième objet de l'invention est une utilisation du procédé de masquage de l'invention pour sécuriser un document de sécurité tel que par exemple un chèque bancaire.

Le premier objet de l'invention est atteint par un procédé de masquage d'une donnée claire b de n bits, caractérisé en ce qu'on produit une donnée masquée m en utilisant la fonction de masquage suivante : $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, où p est un nombre premier, b_i est le bit de rang i de la donnée claire b, q_i est le nombre premier de rang i d'un ensemble de nombres premiers (q_1, ..., q_n). De préférence, p est un nombre premier de grande taille et les éléments de l'ensemble de nombres premiers sont de petite taille.

Par rapport aux fonctions de hachage connues, la fonction $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$ a pour principal intérêt d'être tolérante aux erreurs, comme on le verra mieux par la suite, elle est de ce fait particulièrement bien adaptée pour chiffrer des données biométriques.

Le deuxième objet de l'invention concerne un procédé de masquage d'une empreinte biométrique au cours duquel on détermine un ensemble de s minuties réelles caractéristiques de la dite empreinte, caractérisé en ce qu'ensuite, on mélange et on range les minuties réelles avec t fausses minuties puis on forme une donnée biométrique mélangée b de n = s + t bits telle que, pour tout i :

b_i = 1 si le rang i correspond à une minutie réelle et

b_i = 0 si le rang i correspond à une fausse minutie.

De préférence, après l'étape de mélange, on produit une donnée biométrique chiffrée en chiffrant la donnée biométrique mélangée par un procédé tel que décrit ci-dessus.

Le troisième objet de l'invention concerne quant à lui un procédé de sécurisation d'un document de sécurité, par exemple un chèque bancaire, au cours duquel, après avoir obtenu une donnée de référence par masquage d'une empreinte biométrique selon un procédé tel que décrit ci-dessus,

- on mémorise la dite donnée chiffrée de référence sur ou dans le document de sécurité, ou
- on associe à la dite donnée de référence un code -barre que l'on mémorise sur ou dans le document de sécurité, la donnée de référence et le code -barre étant également mémorisée dans une table.

Des exemples préférés de mise en œuvre de l'invention sont décrits ci-dessous.

On va tout d'abord détailler le procédé de masquage selon l'invention. Pour masquer une donnée claire $b = (b_n, \ldots, b_1)$ de n bits, on utilise la fonction de masquage suivante :

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$$

La fonction utilise comme paramètres un ensemble $(q_n, \ldots, q_1)$ de petits nombres premiers, par exemple des nombres entiers d'environ 60 bits. La fonction utilise également un paramètre p, qui est un entier de grande taille, par exemple d'environ 1024 bits. p est choisi de préférence tel que $2*q_n\text{^}2t < p < 4*q_n\text{^}2t$, où t est un nombre d'erreurs acceptées.

Contrairement aux fonctions de hachage connues, la fonction selon l'invention est peu sensible aux erreurs, c'est-à-dire que, connaissant deux données m, μ chiffrées

par cette fonction, il est possible de dire si les données claires d'origine b, β correspondantes sont identiques, à au maximum t erreurs près.

En effet, m, μ sont obtenues par les relations :

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p \text{ et } \mu = \prod_{i=1}^{n} q_i^{\beta_i} \bmod p,$$

On définit de plus :

$$\lambda = \frac{m}{\mu} \bmod (p) = \frac{a}{\alpha} \bmod p$$

avec $a = \prod_{i \in \Delta_i} q_i \bmod p$ et $\alpha = \prod_{i \in \Gamma_i} q_i \bmod p$

où Δ_i est l'ensemble des indices i compris entre 1 et n pour lesquels $b_i = 1$ et $\beta_i = 0$, et où Γ_i est l'ensemble des indices i compris entre 1 et n pour lesquels $b_i = 0$ et $\beta_i = 1$. La somme des tailles des ensembles Δ_i et Γ_i est au plus égale à t, t étant le nombre de bits de β différents des bits de b de même rang, correspondant au nombre maximum d'erreurs acceptées.

a et α, qui sont des produits de petits nombres de nombres premiers q_i, sont également des petits nombres, qui vérifient de plus la relation : $a*\lambda = \alpha \bmod p$. A partir de cette dernière égalité et du nombre λ, il est alors possible de retrouver les nombres a et α. Une décomposition de a et α en nombres premiers permet finalement factoriser a et α. La décomposition est facilitée en tirant partie du fait que a et α se décomposent en principe en de petits nombres premiers. Si a et α se décomposent sur l'ensemble $(q_n, \ldots, q_1)$, alors on en déduit que les données d'origine b et β sont identiques, à au plus t erreurs près.

On va maintenant décrire un mode préféré de mise en œuvre d'un procédé de masquage d'une empreinte biométrique utilisant la fonction de masquage décrite ci-dessus.

Dans l'exemple ci-dessous, l'empreinte biométrique physique que l'on cherche à masquer est une empreinte digitale caractérisée par un nombre s prédéfini de minutiae réelles. Une minutie réelle est un détail d'une empreinte en un point donné de l'empreinte physique, comme par exemple une rupture d'une ligne, une fourche sur une ligne, etc. Numériquement, une minutie peut être traduite par une chaîne de caractères incluant des informations sur la position et la forme de la minutie.

Selon l'invention, pour masquer l'empreinte physique, on ajoute à l'ensemble des minuties réelles un ensemble de t fausses minuties, également définies par une chaîne de caractères mais qui ne correspondent pas à une minutie réelle de l'empreinte physique. Dans un exemple, une fausse minutie est définie de manière totalement aléatoire, et on ajoute un ensemble de $t = 80$ fausses minuties à un ensemble de $s = 20$ minuties réelles.

L'ordre des minuties réelles et des fausses minutiae est mélangé, par exemple de façon aléatoire, puis on définit un nombre $b = (b_n, \ldots, b_1)$ de $n = s + t$ bits tel que, pour tout i :

$b_i = 1$ si le rang i correspond à une minutie réelle et
$b_i = 0$ si le rang i correspond à une fausse minutie.

Le nombre b est ensuite masqué par la fonction de masquage selon l'invention pour produire une empreinte masquée m telle que :

$$m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$$

L'empreinte masquée peut ensuite être mémorisée dans une base de données, sur une carde d'identité, dans une mémoire d'une carte à puce, etc.

Pour vérifier l'identité d'une personne, il suffira ensuite :

- de relever une empreinte biométrique physique sur la personne puis de calculer l'ensemble de s minuties réelles correspondant,
- de faire correspondre les minutiae de cette nouvelle empreinte avec l'empreinte de référence, de déterminer le nombre β associé, puis de chiffrer le nombre β par la fonction $\mu = \prod_{i=1}^{n} q_i^{\beta_i} \bmod p$,
- de déterminer s'il y a concordance entre la donnée m masquée (l'empreinte masquée de référence) précédemment mémorisée et l'empreinte μ masquée à partir de l'empreinte réelle qui vient d'être relevée.

Pour déterminer s'il y a concordance entre m et μ :

- on calcule $\lambda = \frac{m}{\mu} \bmod p = \frac{a}{\alpha} \bmod p$, puis a et α à partir de la relation $a*\lambda = \alpha \bmod p$, avec a et α petits devant l'entier p, par l'algorithme des fractions continues par exemple.
- on décompose ensuite a et α en facteurs premiers, puis
  - il y a concordance si a et α se décomposent sur au plus t éléments de l'ensemble des nombres premiers $(q_n, \ldots, q_1)$,
  - il n'y a pas concordance sinon

Une application envisagée de l'utilisation des procédés de masquage selon l'invention vise à sécuriser un document de sécurité tel que par exemple un chèque bancaire. Pour cela, selon l'invention :

- une empreinte biométrique du propriétaire du document de sécurité est masquée par un procédé de masquage tel que décrit ci-dessus,
- l'empreinte masquée est associée à un code - barre, et le couple empreinte chiffrée / code - barre associé est mémorisé dans une base de donnée,
- le code - barre est finalement mémorisé, par exemple par impression, sur le document de sécurité.

Il suffit ensuite, lorsque le document de sécurité est transmis par exemple, de prendre simultanément avec le document de sécurité une empreinte biométrique de la personne qui transmet le dit document puis de vérifier que la personne qui transmet le document est bien la personne dont l'empreinte est mémorisée sur le document. La vérification pourra être faite par toute personne ayant accès à la base de données, et qui n'est pas nécessairement la personne qui reçoit le document.

Le code - barre est réalisé selon des techniques connues, on pourra utiliser par exemple un code - barre à une dimension, constitué d'une série de barres verticales d'épaisseur et d'écartement variables. Le choix de la forme du code - barre est en pratique fonction de la taille de l'empreinte chiffrée à mémoriser.

La base de données dans laquelle les couples empreinte masquée / code - barre associé sont mémorisés est accessible pour vérification uniquement à un nombre restreint de personnes, selon le niveau de sécurité

souhaité : l'accès peut par exemple être autorisé pour toute personne amenée à recevoir des documents de sécurité ou, de manière plus restreinte, uniquement à une autorité certificatrice.

Dans un exemple pratique, le document de sécurité est un chèque bancaire et l'empreinte digitale de son propriétaire est mémorisée sur le chèque sous la forme d'un code - barre. Un commerçant dispose d'un dispositif de lecture et de comparaison d'une empreinte doté de moyens pour lire une empreinte, la masquer puis imprimer l'empreinte chiffrée. La banque émettrice du chèque a seul le droit d'accès à la base de données dans laquelle sont mémorisés l'empreinte initiale chiffrée et le code - barre associé ; cet accès lui permet de vérifier que l'empreinte laissée par la personne qui a présenté le chèque au commerçant, et que ce dernier a vérifiée et imprimée sur le chèque, correspond bien à celle du propriétaire du chèque.

REVENDICATIONS

1. Procédé de masquage d'une empreinte biométrique au cours duquel on détermine un ensemble de s minuties réelles caractéristiques de la dite empreinte, caractérisé en ce qu'ensuite, on mélange et on range les minuties réelles avec t fausses minuties puis on forme une donnée biométrique mélangée b de n = s + t bits telle que, pour tout i :

b_i = 1 si le rang i correspond à une minutie réelle et

b_i = 0 si le rang i correspond à une fausse minutie.

2. Procédé selon la revendication 1, dans lequel les minuties réelles et les fausses minuties sont mélangées de façon aléatoire.

3. Procédé selon l'une des revendications 1 à 2, au cours duquel, après l'étape de mélange, on produit une donnée biométrique masquée en masquant la donnée biométrique mélangée en utilisant la fonction de masquage suivante : $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, où p est un nombre premier, b_i est le bit de rang i de la donnée biométrique mélangée b, q_i est le nombre premier de rang i d'un ensemble de nombres premiers (q_1, ..., q_n) et m est la donnée biométrique masquée.

4. Procédé de masquage selon la revendication précédente, dans lequel p est un nombre premier de grande taille et les éléments de l'ensemble de nombres premiers sont de petite taille.

5. Procédé de sécurisation d'un document de sécurité, par exemple un chèque bancaire, au cours duquel, après avoir obtenu une donnée masquée de référence par masquage d'une empreinte biométrique selon un procédé selon la revendication 1 à 4,

- on mémorise la dite donnée masquée de référence sur ou dans le document de sécurité, ou
- on associe à la dite donnée masquée de référence un code - barre que l'on mémorise sur ou dans le document de sécurité, la donnée chiffrée de référence et le code -barre étant également mémorisée dans une table.

6. Procédé de vérification d'un document de sécurité sécurisé par un procédé selon la revendication 5, procédé de vérification au cours duquel :

- on numérise une empreinte biométrique physique d'une personne présentant le document de sécurité,
- on masque l'empreinte numérisée par un procédé selon l'une des revendications 1 à 4,
- on compare l'empreinte numérisée masquée avec la donnée de référence mémorisée sur le document de sécurité, puis
- on accepte le document de sécurité si l'empreinte numérisée et la donnée masquée de référence sont identiques à un taux d'erreur près prédéfini, ou on refuse le titre sinon

7. Procédé selon la revendication précédente, dans lequel, lors de l'étape de comparaison, si un code - barre associé à la donnée chiffrée est mémorisé sur le document de sécurité, alors :

- on lit le code - barre et on recherche dans une table une donnée masquée de référence associée, puis
- on compare la donnée masquée de référence avec l'empreinte numérisée.

8. Procédé de masquage d'une donnée claire b de n bits, procédé susceptible d'être utilisé pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 4, d'un procédé selon l'une des revendications 5 à 6 ou d'un procédé selon la revendication 7, le procédé étant caractérisé en ce qu'on produit une donnée chiffrée m en utilisant la fonction de masquage suivante : $m = \prod_{i=1}^{n} q_i^{b_i} \bmod p$, où p est un nombre premier, b_i est le bit de rang i de la donnée claire b, q_i est le nombre premier de rang i d'un ensemble de nombres premiers (q_1, ..., q_n).

9. Procédé de masquage selon la revendication précédente, dans lequel p est un nombre premier de grande taille et les éléments de l'ensemble de nombres premiers sont de petite taille.

RÉPUBLIQUE FRANÇAISE

2870413

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

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

N° d'enregistrement national

FA 652052
FR 0405236

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	US 6 185 316 B1 (BUFFAM WILLIAM J) 6 février 2001 (2001-02-06) * abrégé * * colonne 11, ligne 58 - colonne 15, ligne 40; figures 1,2 * * colonne 23, ligne 14 - ligne 44 * -----	1,2,5-7	H04L9/32 G06K9/62
A	US 6 697 947 B1 (MATYAS JR STEPHEN MICHAEL ET AL) 24 février 2004 (2004-02-24) * colonne 1, ligne 61 - colonne 2, ligne 27 * * colonne 3, ligne 4 - ligne 67 * * colonne 12, ligne 51 - colonne 14, ligne 10 * -----	3,8	

DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)

H04L
G07C
G06K

Date d'achèvement de la recherche	Examinateur
22 octobre 2004	Carnerero Álvaro, F

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

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0405236 FA 652052

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 22-10-2004
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 6185316 B1	06-02-2001	AUCUN	
US 6697947 B1	24-02-2004	AUCUN	

EPO FORM P0465