(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 3 043 511 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
13.07.2016 Bulletin 2016/28

(51) Int Cl.:
H04L 9/32 *(2006.01)*

(21) Numéro de dépôt: **16150447.7**

(22) Date de dépôt: **07.01.2016**

(84) Etats contractants désignés:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Etats d'extension désignés:
BA ME
Etats de validation désignés:
MA MD

(30) Priorité: **08.01.2015 FR 1550156**

(71) Demandeur: **Morpho**
92130 Issy-les-Moulineaux (FR)

(72) Inventeur: **MOREL, Constance**
92130 ISSY LES MOULINEAUX (FR)

(74) Mandataire: **Regimbeau**
20, rue de Chazelles
75847 Paris Cedex 17 (FR)

(54) PROCÉDÉ D'IDENTIFICATION D'UNE ENTITÉ

(57) La présente invention concerne procédé d'identification d'une entité mis en oeuvre par un système d'identification à partir de données de distance indexées (d_1,...,d_n) correspondant à des entités de référence et comprenant:

- une **phase de détermination** d'un ensemble (I) d'indices de minima ($index_1$, ..., $index_k$) parmi lesdites données de distance indexées binaires de longueur q' comprenant **une étape d'exécution** comprenant,

pour chaque ensemble des $j^{ème}$ bits des données de distance indexées comprises dans une liste de données à traiter, j étant un entier variant de q'-1 à 0, en commençant par l'ensemble des bits de poids fort des données à traiter et en terminant par l'ensemble des bits de poids faible des données à traiter,

la recherche d'indices de minima comprenant, si un nombre d'indices d'un premier groupe d'indices de données de distance indexées (p) est supérieur à un nombre restant de données indexées à écarter (r), un ajout desdits indices d'un deuxième groupe à l'ensemble d'indices de minima;

- **une phase d'identification** de l'entité à identifier parmi les entités de référence correspondant aux données biométriques de références stockées associées aux indices de données de distance minimales ($index_1$, ...$index_k$) déterminés,

les opérations sur des entiers binaires pour la mise en oeuvre d'au moins ladite étape d'exécution, étant traduites sous la forme d'au moins un circuit booléen utilisé pour mettre en oeuvre au moins ladite étape d'exécution de manière sécurisée entre le serveur de contrôle et le serveur de gestion à l'aide d'un protocole de calcul sécurisé multipartite permettant une évaluation sécurisée dudit circuit booléen.

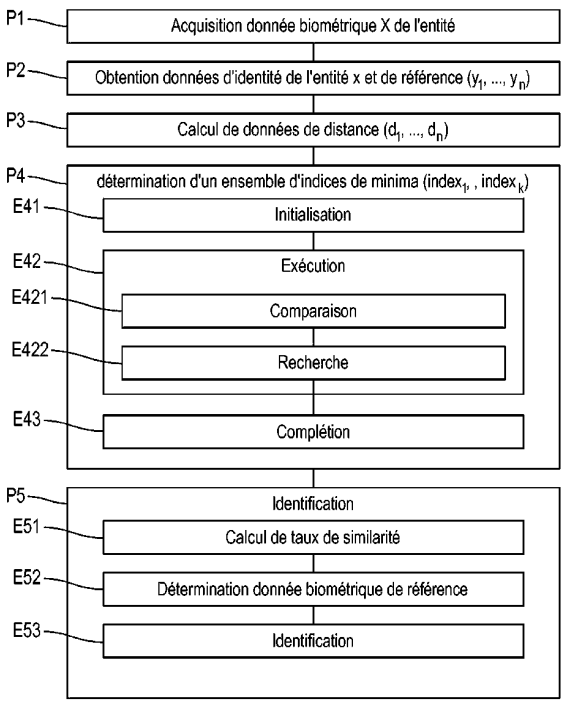

FIG. 2

EP 3 043 511 A1