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

(11) EP 3 200 384 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
02.08.2017 Bulletin 2017/31

(51) Int Cl.:
H04L 9/00 *(2006.01)*

(21) Numéro de dépôt: **17153545.3**

(22) Date de dépôt: **27.01.2017**

(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: **28.01.2016 FR 1650693**

(71) Demandeur: **Safran Identity & Security**
92130 Issy-les-Moulineaux (FR)

(72) Inventeurs:
- **MOREL, Constance**
  92130 ISSY LES MOULINEAUX (FR)
- **BRINGER, Julien**
  92130 ISSY LES MOULINEAUX (FR)
- **CHABANNE, Hervé**
  92130 ISSY LES MOULINEAUX (FR)

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

(54) PROCÉDÉ D'EXECUTION DE CALCUL CRYPTOGRAPHIQUE ET APPLICATION A LA CLASSIFICATION PAR MACHINES A VECTEURS DE SUPPORT

(57) L'invention propose un procédé comprenant le calcul d'une fonction s'écrivant comme un produit de :
- une sous-fonction f_X d'une donnée d'une unité-client
- une sous-fonction f_Y d'une donnée d'une unité-client, et
- un produit de n sous-fonctions indexées f_i des deux données,

le procédé comprenant les étapes de:

- génération aléatoire, par l'unité-serveur, de n données inversibles indexées r_i de l'ensemble $\mathbb{Z}_m$, avec m premier,
- génération, par l'unité-serveur, pour chaque i de 1 à n, d'un ensemble dont chaque élément est formé par le produit d'une donnée r_i avec un résultat possible de la sous-fonction de deux variables f_i évaluée en les deux données,
- mise en oeuvre d'un protocole de transfert inconscient entre l'unité client et l'unité serveur pour que l'unité client récupère, pour chaque i de 1 à n, une donnée intermédiaire t_i égale à :

$$t_i = r_i \times f_i(x_i, Y)$$

- obtention, par l'unité client, d'un résultat T à partir des données intermédiaires tel que :

$$T = f_X(X') \times \prod_{i=1}^{n} t_i$$

- obtention, par l'unité serveur, d'un résultat R à partir des données inversées tel que:

$$R = f_Y(Y) \times \prod_{i=1}^{n} r_i^{-1}$$

- utilisation des résultats T et R dans une application cryptographique.

EP 3 200 384 A1