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

(11) EP 3 200 387 A1

(12) DEMANDE DE BREVET EUROPEEN

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

(51) Int Cl.:
H04L 9/30 *(2006.01)*

(21) Numéro de dépôt: **17153613.9**

(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 1650694**

(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 DE CALCUL SÉCURISÉ MULTIPARTITE PROTÉGÉ CONTRE UNE PARTIE MALVEILLANTE

(57) L'invention propose un procédé comprenant l'évaluation d'une fonction F obtenue par l'application à n sous-fonctions f_i d'une première opération, l'évaluation comprenant:
- la mise en oeuvre d'une série d'étapes de calcul dans lequel une première unité prend un rôle de client et une deuxième unité prend un rôle de serveur, et
- la répétition de la série d'étapes de calcul dans laquelle les rôles de client et de serveur sont échangés entre les unités, chaque série d'étapes comprenant :
a) génération aléatoire, par le serveur, de premières données, et d'une deuxième donnée,
b) pour chaque sous-fonction f_i, génération par le serveur d'un ensemble d'éléments formés par :
o un résultat de f_i évaluée en les données du client et du serveur,
o masqué par une première donnée, par application de la première opération entre le résultat et la première donnée, et
o masqué par la deuxième donnée, par application entre le résultat masqué et la deuxième donnée d'une deuxième opération différente de la première et distributive par rapport à celle-ci,
c) récupération par transfert inconscient, par le client, d'une donnée intermédiaire correspondant à l'un des éléments générés par le serveur,
d) génération, par le serveur, d'une première partie de résultat, par :
• le masquage de chaque première donnée par la deuxième donnée,
• l'application à toutes les premières données masquées de la première opération, et
e) génération, par le client, d'une deuxième partie de résultat, par application à toutes les données intermédiaires de la première opération.

EP 3 200 387 A1

(Cont. page suivante)