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

(11) EP 3 091 689 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
09.11.2016 Bulletin 2016/45

(51) Int Cl.:
H04L 9/00 *(2006.01)* ***H04L 9/32*** *(2006.01)*

(21) Numéro de dépôt: **16168407.1**

(22) Date de dépôt: **04.05.2016**

(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: **06.05.2015 FR 1554077**

(71) Demandeur: **MORPHO**
92130 Issy-Les-Moulineaux (FR)

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

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

(54) PROCÉDÉ DE GÉNÉRATION D'UNE SIGNATURE DE MESSAGE À PARTIR D'UN JETON DE SIGNATURE CHIFFRÉ À L'AIDE D'UNE FONCTION DE CHIFFREMENT HOMOMORPHIQUE

(57) L'invention concerne un procédé de génération d'une signature d'un message destinée à être validée par un serveur vérifieur,
un dispositif client étant configuré pour détenir une clé privée et une clé publique correspondante et comprenant des étapes de :
-calcul (103) préalablement hors ligne par un module matériel de sécurité d'un jeton de signature résultat d'un chiffrement à l'aide d'une fonction de chiffrement homomorphique,
- stockage (104) dudit jeton de signature ;
- génération (105) de ladite signature dudit message chiffrée à l'aide de ladite fonction de chiffrement homomorphique à partir du résultat du chiffrement par ladite fonction de chiffrement homomorphique de la clé privée stockée par le dispositif client, du jeton de signature et dudit message, ladite signature étant destinée à être validée par ledit serveur vérifieur à l'aide de ladite clé publique.

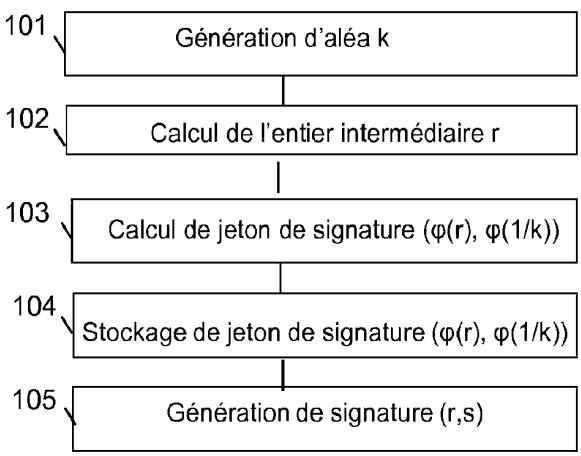

FIG. 2

EP 3 091 689 A1