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

(11) EP 3 211 826 A1

(12) DEMANDE DE BREVET EUROPEEN

(43) Date de publication:
30.08.2017 Bulletin 2017/35

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

(21) Numéro de dépôt: **17157289.4**

(22) Date de dépôt: **22.02.2017**

(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: **25.02.2016 FR 1651549**

(71) Demandeur: **Commissariat à l'Energie Atomique et aux Energies Alternatives**
75015 Paris (FR)

(72) Inventeur: **SAVRY, Olivier**
38360 Sassenage (FR)

(74) Mandataire: **Brevalex**
56, Boulevard de l'Embouchure
B.P. 27519
31075 Toulouse Cedex 2 (FR)

(54) MÉTHODE DE GESTION DE CERTIFICATS IMPLICITES AU MOYEN D'UNE INFRASTRUCTURE À CLÉS PUBLIQUES DISTRIBUÉE

(57) L'invention concerne une méthode de gestion de certificats implicites d'un chiffrement sur courbe elliptique (ECQV). Les certificats implicites sont stockés dans différents noeuds du réseau en fonction d'une table de hachage distribuée (DHT) et non auprès d'une autorité de certification unique. Le certificat implicite de la clé publique associée à un noeud est obtenu en chaînant des opérations de certification élémentaires auprès d'une suite de noeuds indexeurs du réseau. Le chainage des opérations de certification élémentaires permet de renforcer l'authentification des noeuds du réseau.

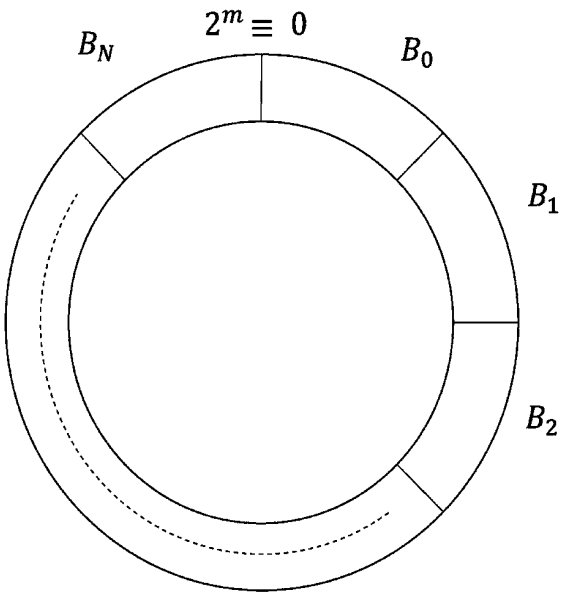

Fig. 1

EP 3 211 826 A1

(Cont. page suivante)