



(43) Date de la publication internationale
5 juillet 2012 (05.07.2012)

WIPO | PCT

(10) Numéro de publication internationale
WO 2012/089632 A1

(51) Classification internationale des brevets :
H04L 9/32 (2006.01) H04L 9/06 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2011/073873

(22) Date de dépôt international :
22 décembre 2011 (22.12.2011)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
1005185 30 décembre 2010 (30.12.2010) FR

(71) Déposant (pour tous les États désignés sauf US) :
THALES [FR/FR]; 45 rue de Villiers, F-92200 Neuilly
Sur Seine (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : PAIN-
CHAULT, Philippe [FR/FR]; 160 boulevard de Valmy, F-
92700 Colombes (FR). GARRIDO, Eric [FR/FR]; 160
boulevard de Valmy, F-92700 Colombes (FR). MARCEL-
LO, Sandra [FR/FR]; 160 boulevard de Valmy, F-92700
Colombes (FR).

(74) Mandataires : DUDOUIT, Isabelle et al.; Immeuble Vi-
sium, 22 Avenue Aristide Briand, F-94117 Arcueil (FR).

(81) États désignés (sauf indication contraire, pour tout titre
de protection nationale disponible) : AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,
KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR,
TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés (sauf indication contraire, pour tout titre
de protection régionale disponible) : ARIPO (BW, GH,
GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ,
UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU,
TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, ML, MR, NE, SN, TD, TG).

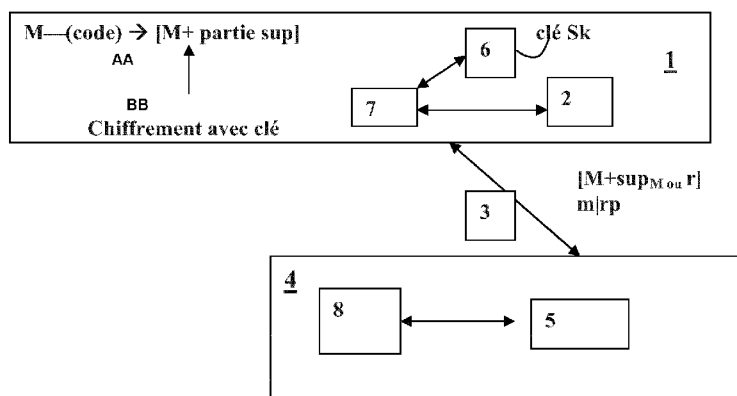
Publiée :

— avec rapport de recherche internationale (Art. 21(3))

(54) Title : METHOD AND SYSTEM MAKING IT POSSIBLE TO TEST A CRYPTOGRAPHIC INTEGRITY OF AN ERROR
TOLERANT DATA ITEM

(54) Titre : PROCEDE ET SYSTEME PERMETTANT DE TESTER UNE INTEGRITE CRYPTOGRAPHIQUE D'UNE DON-
NEE TOLERANTE AUX ERREURS

FIG.1



AA [M + Sup part]
6 Key Sk
BB encryption with key
3 [M + Sup m or r]

(57) Abstract : Method and system for testing the
cryptographic integrity of data m comprising at
least the following elements a module (1) emitting
a message M, said module comprising a memory
(2) making it possible to store the parameters used
to execute the steps of the method according to
the invention, such as the key, the public data,
which will be explained hereinafter, a transmis-
sion medium (3), a receiver module (4) also com-
prising means (5) for storing at least the same pa-
rameters as at emission. The system can comprise
means (6) for storing confidential data such as the
secret keys, a processor (7) suitable for executing
the steps.

(57) Abrégé : Procédé et système pour tester l'in-
tégrité cryptographique de données m comprenant
au moins les éléments suivants un module (1)
émetteur d'un message M, ledit module compren-
ant une mémoire (2) permettant de stocker les
paramètres utilisés pour exécuter les étapes du
procédé selon l'invention, tels que la clé, les don-
nées publiques, qui seront explicités ci-après, un
médium (3) de transmission, un module récepteur
(4) comprenant aussi des moyens de stockage (5)
d'au moins les mêmes paramètres qu'à l'émission.

Le système peut comprendre des moyens de stockage (6) de données confidentielles telles que les clés secrètes, un processeur (7)
adapté à exécuter les étapes.