



(51) Classification internationale des brevets :
H04L 9/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2010/061350

(22) Date de dépôt international :
4 août 2010 (04.08.2010)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
09/03845 4 août 2009 (04.08.2009) 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) : DUPREZ,
Adrien [FR/FR]; 160, boulevard de Valmy, BP. 82,
F-92704 Colombes Cedex (FR). GOMPEL, Paul
[FR/FR]; 160, boulevard de Valmy, BP. 82, F-92704
Colombes Cedex (FR). PAINCHAULT, Philippe
[FR/FR]; 160, boulevard de Valmy, BP. 82, F-92704
Colombes Cedex (FR).

(74) Mandataires : LUCAS, Laurent et al.; Immeuble
Visium, 22, avenue Aristide Briand, F-94117 ARCUEIL
Cedex (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, RO, RS, RU, 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, 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, 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))

[Suite sur la page suivante]

(54) Title : METHOD FOR GENERATING CRYPTOGRAPHIC HALF-KEYS, AND ASSOCIATED SYSTEM

(54) Titre : PROCEDE DE GENERATION DE DEMI-CLES CRYPTOGRAPHIQUES ET SYSTEME ASSOCIE

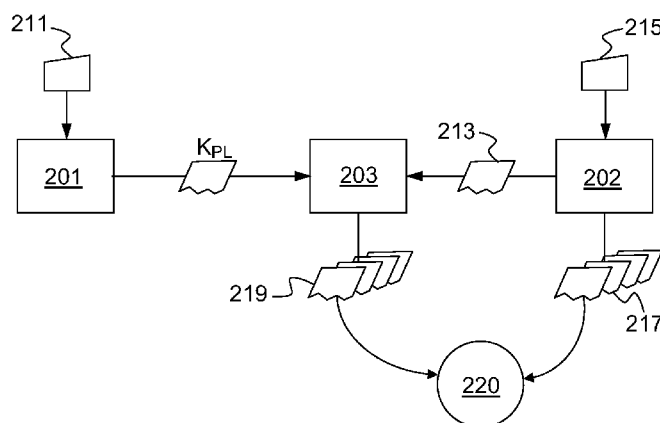


FIG.2

(57) Abstract : The present invention relates to a method for generating cryptographic half-keys. The method enables the generation of n pairs (K_1^i, K_2^i) , wherein $1 \leq i \leq n$, of cryptographic half-keys, each of said pairs enabling the reconstruction of an access key K_{PL} specific to a secure apparatus, said method including at least the following steps: from a separate management center for said apparatus, generating (202) and recording a first series (217) of n half-keys K_1^i on a recording medium (213); supplying (203) the apparatus with said recording medium (213) in order to generate, from said local key K_{PL} and the n half-keys K_1^i stored on said medium, a second series of n half-keys K_2^i so as to form said n pairs (K_1^i, K_2^i) . The invention can be used in particular for creating a plurality of access keys to a secure apparatus.

(57) Abrégé :

[Suite sur la page suivante]

