



- (51) Classification internationale des brevets :
H04N 21/438 (2011.01) H04N 21/4623 (2011.01)
- (21) Numéro de la demande internationale :
PCT/EP2014/064332
- (22) Date de dépôt international :
4 juillet 2014 (04.07.2014)
- (25) Langue de dépôt : français
- (26) Langue de publication : français
- (30) Données relatives à la priorité :
13177287.3 19 juillet 2013 (19.07.2013) EP
- (71) Déposant : NAGRAVISION S.A. [CH/CH]; Route de Genève 22-24, CH-1033 Cheseaux-sur-Lausanne (CH).
- (72) Inventeurs : MACCHETTI (IT), Marco; Via Boccaccio 42, I-22070 Casnate con Bernate (IT). PERRINE, Jérôme; Rue de la Poste 3, CH-1122 Romanel sur Morges (CH). SERVET, Patrick; ch. de Sous-le-Mont 38, CH-1033 Cheseaux-sur-Lausanne (CH). HUNACEK, Didier; ch. du Pré des Planches 16C, CH-1807 Blonay (CH).
- (74) Mandataire : LEMAN CONSULTING S.A. 284; Chemin de Précossy 31, CH-1260 Nyon (CH).
- (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, BN, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, 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,

[Suite sur la page suivante]

(54) Title : METHOD FOR PROTECTING DECRYPTION KEYS IN A DECODER AND DECODER FOR IMPLEMENTING SAID METHOD

(54) Titre : METHODE POUR LA PROTECTION DE CLES DE DECHIFFREMENT DANS UN DECODEUR ET DECODEUR POUR LA MISE EN OEUVRE DE CETTE METHODE

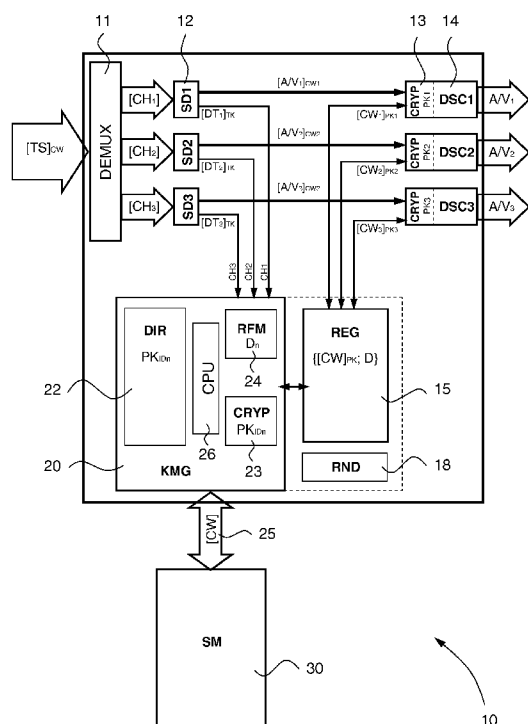


Fig. 1

(57) Abstract : The invention relates to a method for securing control words (CW) within a decoder (10) responsible for unscrambling digital content protected by those control words, comprising the following steps: - for each unscrambling unit (14) of said decoder, loading a pairing key (PK) referenced by an identifier (ID) associating it with an unscrambling unit into a directory (22), - receiving at least one encrypted control word referenced by an indication making it possible to identify the unscrambling unit for which it is intended, - decrypting the control word using a first key shared with a security module (30), - identifying, in the log, the pairing key whose identifier (ID) corresponds to the indication of intended use (D) associated with the control word, - encrypting that control word using that pairing key, - storing the control word in a log (15) in a chronological and referenced manner.

(57) Abrégé : Méthode pour sécuriser des mots de contrôle (CW) au sein d'un décodeur (10) en charge de désambrouiller un contenu numérique protégé par ces mots de contrôle, comprenant les étapes suivantes: - pour chaque unité de désambrouillage (14) que compte ce décodeur, charger dans un répertoire (22), une clé d'appariement (PK) référencée par un identifiant (ID) l'associant à une

[Suite sur la page suivante]



TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, **Publiée :**
KM, ML, MR, NE, SN, TD, TG).

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

unité de désembrouillage, - réceptionner au moins un mot de contrôle chiffré et référencé par une indication (D) permettant d'identifier l'unité de désembrouillage à qui il est destiné, - déchiffrer le mot de contrôle au moyen d'une première clé partagée avec un module de sécurité (30), - identifier dans le répertoire la clé d'appariement dont l'identifiant (ID) correspond à l'indication de destination (D) associée au mot de contrôle, - chiffrer ce mot de contrôle à l'aide de cette clé d'appariement, - stocker dans un registre (15) le mot de contrôle d'une manière chronologique et référencée.