

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
8 avril 2004 (08.04.2004)

PCT

(10) Numéro de publication internationale  
**WO 2004/030363 A1**

(51) Classification internationale des brevets<sup>7</sup> :  
**H04N 7/167, 5/00**

(74) Mandataire : **LEMAN CONSULTING SA**; Route de  
Clémenty 62, CH-1260 Nyon (CH).

(21) Numéro de la demande internationale :  
PCT/IB2003/004121

(81) États désignés (*national*) : AE, AG, AL, AM, AT, AU, AZ,  
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,  
DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH,  
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,  
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,  
MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC,  
SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA,  
UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) Date de dépôt international :  
19 septembre 2003 (19.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :  
2002 1623/02 27 septembre 2002 (27.09.2002) CH  
2002 2048/02 4 décembre 2002 (04.12.2002) CH

(84) États désignés (*régional*) : brevet ARIPO (GH, GM, KE,  
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet  
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet  
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,  
FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,  
TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,  
GW, ML, MR, NE, SN, TD, TG).

(71) Déposant (*pour tous les États désignés sauf US*) :  
**NAGRAVISION SA** [CH/CH]; Route de Genève 22,  
CH-1033 Cheseaux-sur-Lausanne (CH).

Publiée :

— avec rapport de recherche internationale

(72) Inventeurs; et

(75) Inventeurs/Déposants (*pour US seulement*) : **NAHUM,**  
**Sylvain-Victor** [FR/CH]; Avenue de l'Amandolier 24,  
CH-1208 Genève (CH). **STRANSKY, Philippe** [CH/CH];  
Chemin des Grands-Champs, CH-1033 Cheseaux-sur-Lau-  
sanne (CH).

*En ce qui concerne les codes à deux lettres et autres abrégia-  
tions, se référer aux "Notes explicatives relatives aux codes et  
abréviations" figurant au début de chaque numéro ordinaire de  
la Gazette du PCT.*

(54) Title: **CONDITIONAL ACCESS DATA DECRYPTING SYSTEM**

(54) Titre : **SYSTÈME DE DÉCHIFFREMENT DE DONNÉES À ACCÈS CONDITIONNEL**

(57) **Abstract:** The invention concerns a conditional access data decrypting system, in particular for use in pay digital television broadcast. Said system comprises a broadcasting center (1) designed to broadcast encrypted data by control words (cw), at least one management center (11) designed to broadcast personal messages (ECM, EMM) concerning access rights to the encrypted data and to manage said access rights, an operating device (12) for making said encrypted data usable, and a decoder (13) for decrypting at least part of the encrypted data. Said decoder is located between the broadcasting center (10) and the operating device (12). Said decoder (13) consists of a module for receiving (14) the encrypted data and a module for managing (15) access rights to said data. The reception module (14) is connected to or integral with the operating device (12) and the management module (15) is designed to communicate with the reception module. The management module (15) comprises a security module (16) designed to verify the content of the personal messages (ECM, EMM) and to allow or prevent decryption of the control words (cw) on the basis of the personal messages. The reception module receives the encrypted data from the broadcasting center (10) and the management module receives the enabling messages (EMM) from the management center (11).

(57) **Abrégé :** La présente invention concerne un système de déchiffrement de données à accès conditionnel, en particulier utilisé dans le domaine de la télévision numérique à péage. Ce système comporte un centre de diffusion (10) agencé pour diffuser des données chiffrées par des mots de contrôle (cw), au moins un centre de gestion (11) agencé pour diffuser des messages personnels (ECM, EMM) relatifs aux droits d'accès aux données chiffrées et pour gérer ces droits d'accès, un dispositif d'exploitation (12) destiné à rendre utilisables lesdites données chiffrées, et un décodeur (13) agencé pour déchiffrer au moins une partie des données chiffrées. Ce décodeur est placé entre le centre de diffusion (10) et le dispositif d'exploitation (12). Ce décodeur (13) est formé d'un module de réception (14) des données chiffrées et d'un module de gestion (15) des droits d'accès à ces données. Le module de réception (14) est connecté ou intégré au dispositif d'exploitation (12) et le module de gestion (15) est agencé pour communiquer avec le module de réception. Le module de gestion (15) comporte un module de sécurité (16) agencé pour vérifier le contenu des messages personnels (ECM, EMM) et pour permettre ou empêcher le déchiffrement des mots de contrôle (cw) en fonction du contenu des messages personnels. Le module de réception reçoit les données chiffrées provenant du centre de diffusion (10) et le module de gestion reçoit les messages d'autorisation (EMM) du centre de gestion (11).

WO 2004/030363 A1