

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
07 October 2021 (07.10.2021)



(10) International Publication Number
WO 2021/198035 A1

(51) International Patent Classification:

G06F 21/79 (2013.01) G06F 21/55 (2013.01)
G06F 21/64 (2013.01)

(21) International Application Number:

PCT/EP2021/057819

(22) International Filing Date:

25 March 2021 (25.03.2021)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

20167097.3 31 March 2020 (31.03.2020) EP

(71) Applicant: NAGRAVISION S.A. [CH/CH]; 22-24, route de Genève, 1033 Cheseaux-sur-Lausanne (CH).

(72) Inventors: HAUTIER, Roan; C/o Nagravision S.A., Route de Genève 22-24, 1033 Cheseaux-sur-Lausanne (CH). VILLEGAS, Karine; C/o Nagravision S.A., 22-24 route de Genève, 1033 Cheseaux-sur-Lausanne (CH).

(74) Agent: NOVAGRAAF INTERNATIONAL SA et al.; Chemin de l'Echo 3, 1213 Onex (CH).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): 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, DJ, DK, DM, DO,

DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (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, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD FOR SECURELY PROCESSING DIGITAL INFORMATION IN A SECURE ELEMENT

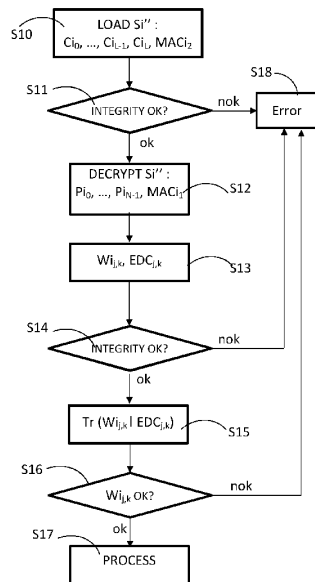


FIG. 6

(57) Abstract: The method for securely processing digital information, has the following steps, performed by a secure element (100) having a secure processor (102): - loading (S10) the digital information (Si'') from an external memory (200) into the secure element (100); - segmenting (S13) the digital information (Si) into words of digital information (Wij,k), generating error-detection codes (EDCj,k) or error-correction codes (ECCi,k) from said words of digital information and associating said error-detection codes with the corresponding words; - transferring (S15) the words of digital information (Wij,k) and the associated error-detection codes (EDCj,k) or error-correction codes (ECCi,k) to the secure processor (102); - in the secure processor (102), verifying (S16) the words of digital information (Wij,k) based on the associated error-detection codes (EDCj,k) or error-correction codes (ECCi,k) before processing the digital information contained in said words (Wij,k).

WO 2021/198035 A1