# (19) World Intellectual Property Organization

International Bureau





# (43) International Publication Date 27 November 2008 (27.11.2008)

PCT

# (10) International Publication Number WO 2008/142612 A3

(51) International Patent Classification: *H04L 9/06* (2006.01) *H04L 9/08* (2006.01)

(21) International Application Number:

PCT/IB2008/051902

(22) International Filing Date: 14 May 2008 (14.05.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 07108581.5

22 May 2007 (22.05.2007) EP

(71) Applicant (for all designated States except US): KONIN-KLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants (for US only): GORISSEN, Paulus, M., H., M., A. [NL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL). MICHIELS, Wilhelmus, P., A., J. [NL/NL]; c/o High Tech Campus

Building 44, NL-5656 AE Eindhoven (NL). **BIJSTER-VELD, Marcel, L., L.** [NL/NL]; c/o High Tech Campus Building 44, NL-5656 AE Eindhoven (NL).

(74) Agents: UITTENBOGAARD, Frank et al.; High Tech Campus Building 44, NL-5656 AE Eindhoven (NL).

(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, BR, BW, BY, BZ, CA, CH, 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, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

#### (54) Title: UPDATING CRYPTOGRAPHIC KEY DATA

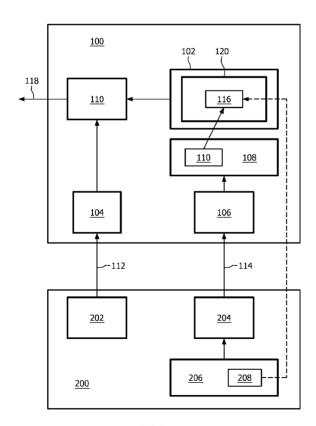


FIG. 1

(57) Abstract: A system 100 for updating cryptographic key data 120 comprises a key input 106 for receiving sequential key updates 114; and a key data updater 108 for changing a portion (116) of the cryptographic key data in response to a received one of the sequential key updates (114), the portion not including all the cryptographic key data, wherein different respective portions of the cryptographic key data are selected for respective ones of the sequential key updates. The system further comprises a content input 104 for receiving content data 112 to be processed; and a cryptographic unit 110 for cryptographic processing of the content data in dependence on the key data to obtain processed content data 118. The content input is arranged for receiving a content data stream, successive portions of the content data stream being encrypted based on successive keys corresponding to the successive key updates.



## WO 2008/142612 A3



European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

#### **Declaration under Rule 4.17:**

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

#### Published:

- with international search report
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments
- (88) Date of publication of the international search report: 5 March 2009

#### INTERNATIONAL SEARCH REPORT

International application No PCT/IB2008/051902

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L9/06 ADD. H04L9/08 According to International Patent Classification (IPC) or to both national classification and IPC **B. FIELDS SEARCHED** Minimum documentation searched (classification system followed by classification symbols) H04L Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal C. DOCUMENTS CONSIDERED TO BE RELEVANT Citation of document, with indication, where appropriate, of the relevant passages Relevant to claim No. PLASMANS, M.: "White-Box Cryptography for X 1 - 15Digital Contents Protection" MASTER'S THESIS, TECHNISCHE UNIVERSITEIT EINDHOVEN, DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, May 2005 (2005-05), XP002508521 Eindhoven Section 6.2 X US 5 404 403 A (BRIGHT MICHAEL W [US] ET 1-4,9-15 AL) 4 April 1995 (1995-04-04) column 1, line 14 - column 2, line 6 column 2, line 38 - column 3, line 9 Further documents are listed in the continuation of Box C. See patent family annex. Special categories of cited documents: "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the 'A' document defining the general state of the art which is not considered to be of particular relevance earlier document but published on or after the international "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone filing date document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such docudocument referring to an oral disclosure, use, exhibition or ments, such combination being obvious to a person skilled in the art. document published prior to the international filing date but later than the priority date claimed \*&\* document member of the same patent family Date of the actual completion of the international search Date of mailing of the international search report 17 December 2008 07/01/2009 Name and mailing address of the ISA/ Authorized officer European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016

Liebhardt, Ingo

## INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/051902

		PCT/IB2008/051902			
C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT					
Category* Δ	Citation of document, with indication, where appropriate, of the relevant passages  CHOW S FT AI: "White-hox cryptography and	Relevant to claim No.			
A	CHOW S ET AL: "White-box cryptography and an AES implementation" 20030101; 20030000, 1 January 2003 (2003-01-01), pages 250-270, XP002462505 cited in the application the whole document	1-15			

#### INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2008/051902

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5404403 A	04-04-1995	NONE	
			•
l			