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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 September 2011 (29.09.2011)

PCT

(10) International Publication Number
WO 2011/119985 A3

(51) International Patent Classification:
G06F 7/04 (2006.01) *G06F 12/00* (2006.01)

(21) International Application Number:
PCT/US2011/030033

(22) International Filing Date:
25 March 2011 (25.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

61/318,220	26 March 2010 (26.03.2010)	US
61/318,744	29 March 2010 (29.03.2010)	US
61/319,198	30 March 2010 (30.03.2010)	US
61/372,390	10 August 2010 (10.08.2010)	US

(71) Applicant *(for all designated States except US)*: **MAXLINEAR, INC.** [US/US]; 2051 Palomar Airport Road, Suite 100, Carlsbad, California 92011-1462 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LECLERCQ, Maxime** [FR/US]; 1232 Hygeia Avenue, Encinitas, California 92024 (US).

(74) Agents: **TABIBI, Ardeshir** et al.; Kilpatrick Towsend & Stockton LLP, Two Embarcadero Center, Eighth Floor, San Francisco, California 94111-3834 (US).

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

Published:

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

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

[Continued on next page]

(54) Title: FIRMWARE AUTHENTICATION AND DECIPHERING FOR SECURE TV RECEIVER

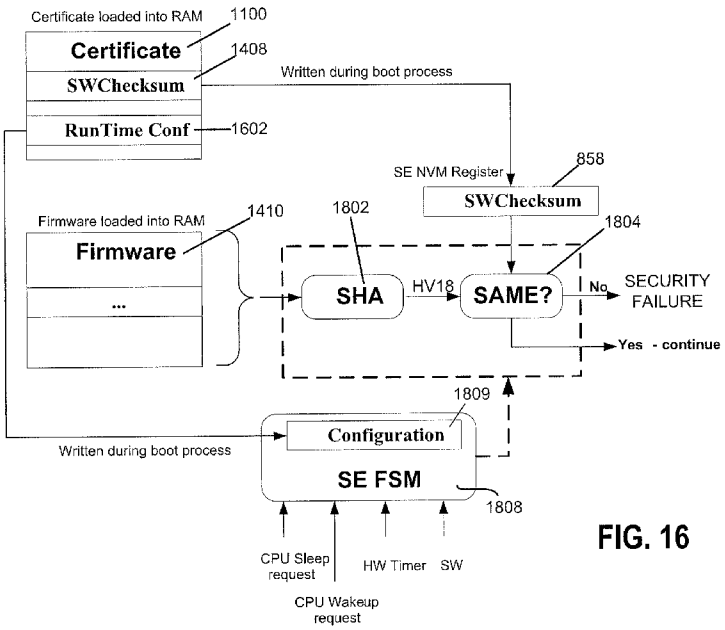

FIG. 16

(57) Abstract: A method for authenticating and deciphering an encrypted program file for execution by a secure element includes receiving the program file and a digital certificate that is associated with the program file from an external device. The method stores the program file and the associated certificate in a secure random access memory disposed in the secure element and hashes the program file to obtain a hash. The method authenticates the program file by comparing the obtained hash with a checksum that is stored in the certificate. Additionally, the method writes runtime configuration information stored in the certificate to corresponding configuration registers disposed in the secure element. The method further generates an encryption key using a seed value stored in the certificate and a unique identifier disposed in the secure element and deciphers the program file using the generated encryption key.

WO 2011/119985 A3

(88) Date of publication of the international search report:
29 December 2011

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 11/30033

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 7/04, G06F 12/00 (2011.01)
USPC - 726/18
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)
IPC(8)- G06F 7/04, G06F 12/00 (2011.01);
USPC- 726/18

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC- 726/2-5, 16-18; 705/50; 700/1,90;
Patents and NPL (classification, keyword; search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWest (US Pat, PgPub, EPO, JPO), GoogleScholar (PL, NPL), FreePatentsOnline (US Pat, PgPub, EPO, JPO, WIPO, NPL); search terms: authenticae, decipher, demodulate, decode, program, firmware, image, file, code, secure, execute, hash, memory, random, acces, public, private, key, root, digest, verify, validate, seed, checksum, signature, certificate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2004/0044906 A1 (ENGLAND et al.) 04 March 2004 (04.03.2004), para [0017], [0019], [0027]-[0029], [0033]-[0045], [0047], [0049], [0054]-[0058], [0060], [0063], [0064]	1-32
Y	US 2007/0192610 A1 (CHUN et al.) 16 August 2007 (16.08.2007), para [0006]-[0008], [0023], [0025], [0029], [0031], [0035]-[0047], [0054], [0055], [0058], [0063]	1-32
Y	US 2009/0094597 A1 (MOSKALIK, et al.) 09 April 2009 (09.04.2009), para [0025]-[0055]	1-32
Y	US 2006/0015731 A1 (LAKSHMI) 19 January 2006 (19.01.2006), para [0025]-[0070]	1-32
Y	US 2004/0025010 A1 (AZEMA et al.) 05 Feburary 2004 (05.02.2004), para [0034]-[0125]	1-32
Y	US 6,424,717 B1 (PINDER et al.) 23 July 2002 (23.07.2002) col 4-42	1-32

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" 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)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"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 invention
"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
"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 documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 October 2011 (26.10.2011)	08 NOV 2011
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)