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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 August 2009 (13.08.2009)

PCT

(10) International Publication Number
WO 2009/100249 A3

(51) International Patent Classification:
G06F 13/14 (2006.01) *G06F 9/00* (2006.01)
G06F 3/00 (2006.01)

(21) International Application Number:
PCT/US2009/033269

(22) International Filing Date:
5 February 2009 (05.02.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/026,438 5 February 2008 (05.02.2008) US

(71) Applicant *(for all designated States except US)*: **VIASAT, INC.** [US/US]; 6155 El Camino Real, Carlsbad, CA 92009 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **OWENS, John, R.** [US/US]; 1928 High Ridge Avenue, Carlsbad, CA 92008 (US). **ANDOLINA, John, C.** [US/US]; 1981 Pinewood Road, Vista, CA 92081 (US). **SHANKEN, Stuart** [US/US]; 5028 Almondwood Way, San Diego, CA 92130 (US). **QUINTANA, Richard, L.** [US/US]; 6482 Kite Place, Carlsbad, CA 92011 (US).

(74) Agents: **FRANKLIN, Thomas, D.** et al.; Townsend And Townsend And Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 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, 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, ST, 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), European (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, SE, SI, SK, 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))*

[Continued on next page]

(54) Title: TRUSTED FIELD-PROGRAMMABLE LOGIC CIRCUITRY

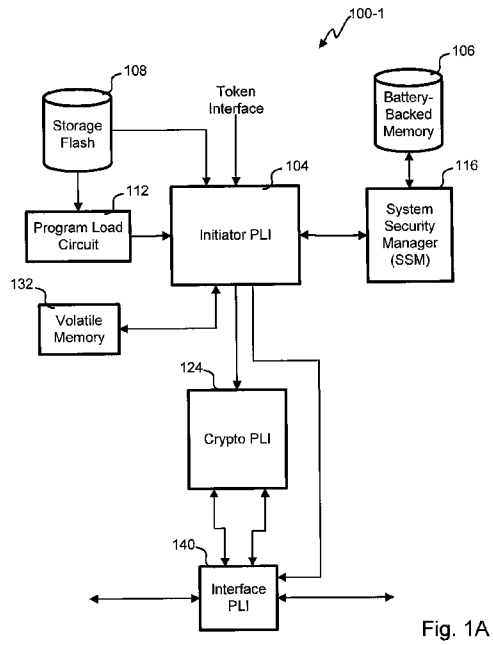

Fig. 1A

(57) Abstract: In one embodiment, a method for trusted booting of a cryptographic processor system is disclosed. Default image(s) is loaded into a field-programmable logic chip (FPLC). The default image(s) cannot perform cryptographic processing, but can perform a first algorithm that is unclassified. A processor, internal or external to the FPLC, can be used with the default image. A multi-layer or multi-part key has portions stored in two different places. A protected image is decrypted with the multi-layer key using the first algorithm and loaded into the FPLC. Cryptographic processing is performed using a second algorithm classified or produced by the government. In another embodiment, a method for securing a field-programmable logic chip (FPLC) is disclosed. Information is cryptographically processed within the FPLC. An error condition is detected outside of the FPLC and the error condition is communicated to the FPLC to disrupt an image(s) within the FPLC. Optionally, at least a portion of a key can be erased such that cryptographic processing is curtailed or eliminated. In yet another embodiment, a method for operating a field-programmable logic chip (FPLC) is disclosed. Operation of the FPLC includes a configuration state and a cryptographic processing state. Switching between states is controlled by a state machine. Each state has one or more images. Transferring between states causes some or all images from the other state being overwritten.

WO 2009/100249 A3

— *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))*

(88) Date of publication of the international search report:
26 November 2009

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/033269

A. CLASSIFICATION OF SUBJECT MATTER

G06F 13/14(2006.01)i, G06F 3/00(2006.01)i, G06F 9/00(2006.01)i

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)

IPC8: G06F09, G06F21, G09C01, H04L09

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility Models and applications for Utility Models since 1975

Japanese Utility Models and application for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS(KIPO internal) "field, programmable, logic, circuit, security, booting, encrypt, decrypt, key, multi-layered, chip, algorithm"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2002-0150252 A1 (DALE WONG) 17 October 2002. See paragraphs [0016] - [0033]; figures 1-6.	1-69
A	US 2006-0265603 A1 (IAN MCLEAN et al.) 23 November 2006. See paragraphs [0022] - [0055]; figures 1-10.	1-69
A	US 2007-0220369 A1 (CAMIL FAYAD et al.) 20 September 2007. See paragraphs [0020] - [0038]; figures 1-4.	1-69
A	US 2006-0059369 A1 (CAMIL FAYAD et al.) 16 March 2006. See paragraphs [0042] - [0070]; figures 1-10.	1-69

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

☒ See patent family annex.

* 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 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
29 SEPTEMBER 2009 (29.09.2009)	**30 SEPTEMBER 2009 (30.09.2009)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer KIM Jong Kee Telephone No. 82-42-481-8301

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/033269

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002-0150252 A1	17.10.2002	None	
US 2006-0265603 A1	23.11.2006	GB 0506117 D0	04.05.2005
		GB 2424557 A	27.09.2006
		JP 2006-295916 A	26.10.2006
US 2007-0220369 A1	20.09.2007	None	
US 2006-0059369 A1	16.03.2006	WO 2006-027309 A1	16.03.2006