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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 October 2015 (15.10.2015)

WIPO | PCT

(10) International Publication Number
WO 2015/157131 A3

(51) International Patent Classification:
*G06F 21/57* (2013.01)

(21) International Application Number:
PCT/US2015/024407

(22) International Filing Date:
5 April 2015 (05.04.2015)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/976,491 7 April 2014 (07.04.2014) US
14/267,894 1 May 2014 (01.05.2014) US

(71) Applicant: **QUALCOMM INCORPORATED** [US/US]; ATTN: International IP Administration, 5775 Morehouse Drive, San Diego, California 92121-1714 (US).

(72) Inventors: **ELNEKAVEH, Or**; 5775 Morehouse Drive, San Diego, California 92121 (US). **KAHANA, Yoni**; 5775 Morehouse Drive, San Diego, California 92121 (US). **KAROLITSKY, Adi**; 5775 Morehouse Drive, San Diego, California 92121 (US).

(74) Agents: **WIGMORE, Steven P.** et al.; Smith Risley Tempel Santos LLC, Two Ravinia Drive, Suite 700, Atlanta, Georgia 30346 (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, BN, 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, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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, 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).

*[Continued on next page]*

(54) Title: SYSTEM AND METHOD FOR BOOT SEQUENCE MODIFICATION USING CHIP-RESTRICTED INSTRUCTIONS RESIDING ON AN EXTERNAL MEMORY DEVICE

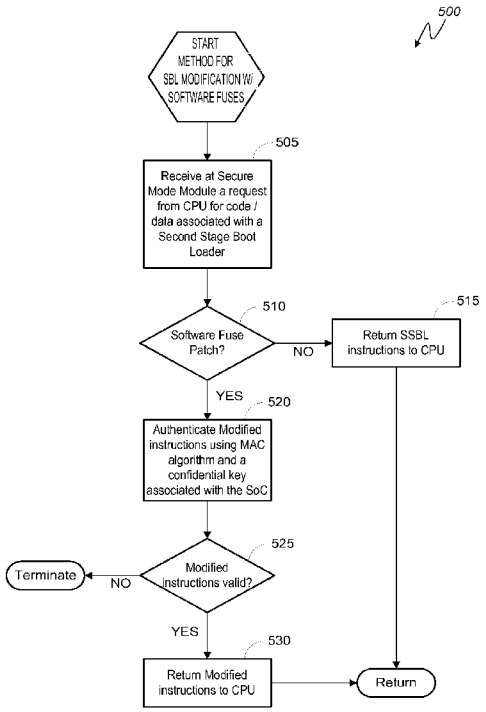


FIG. 5

(57) Abstract: Various embodiments of methods and systems for modification of instructions and/or data associated with one or more boot stages in a boot sequence are disclosed. The authenticity and integrity of the modified instructions and/or data in certain embodiments may be ensured by using a confidential key and a message authentication code ("MAC") algorithm to generate a MAC output. The MAC output is compared to an expected MAC associated with the modified instructions and/or data. The confidential key is uniquely associated with the system on a chip ("SoC") or a component of the SoC. In this way, embodiments of the solution guard against unauthorized modification or replacement of the OEM boot instructions.

WO 2015/157131 A3

**Declarations under Rule 4.17**:

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

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

**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))*

**(88) Date of publication of the international search report**:
17 March 2016

# INTERNATIONAL SEARCH REPORT

International application No
PCT/US2015/024407

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/57
ADD.

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)
G06F

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 practicable, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2012/210115 A1 (PARK DONG-JIN [KR] ET AL) 16 August 2012 (2012-08-16)<br>paragraph [0071]<br>paragraph [0076]<br>paragraph [0079]<br>paragraph [0093]<br>----- | 1-30 |

☐ 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 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 |
|---|---|
| 21 January 2016 | 29/01/2016 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Ebert, Werner |

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2015/024407

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2012210115 A1 | 16-08-2012 | KR 20120092222 A | 21-08-2012 |
| | | US 2012210115 A1 | 16-08-2012 |