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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 March 2013 (21.03.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/040475 A1

(51) International Patent Classification:
G06F 21/00 (2013.01)

(21) International Application Number:
PCT/US2012/055601

(22) International Filing Date:
14 September 2012 (14.09.2012)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/535,047 15 September 2011 (15.09.2011) US

(71) Applicant *(for all designated States except US)*: **CUBIC CORPORATION** [US/US]; 9333 Balboa Avenue, San Diego, California 92123 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BERENBERG, Paul** [US/US]; 773 Bond Way, Mountain View, California 94040 (US). **DANIELYAN, Georgi** [AM/AM]; 51 St. Arabkir, Building 9, Apt. 54, Yerevan, 0014 (AM).

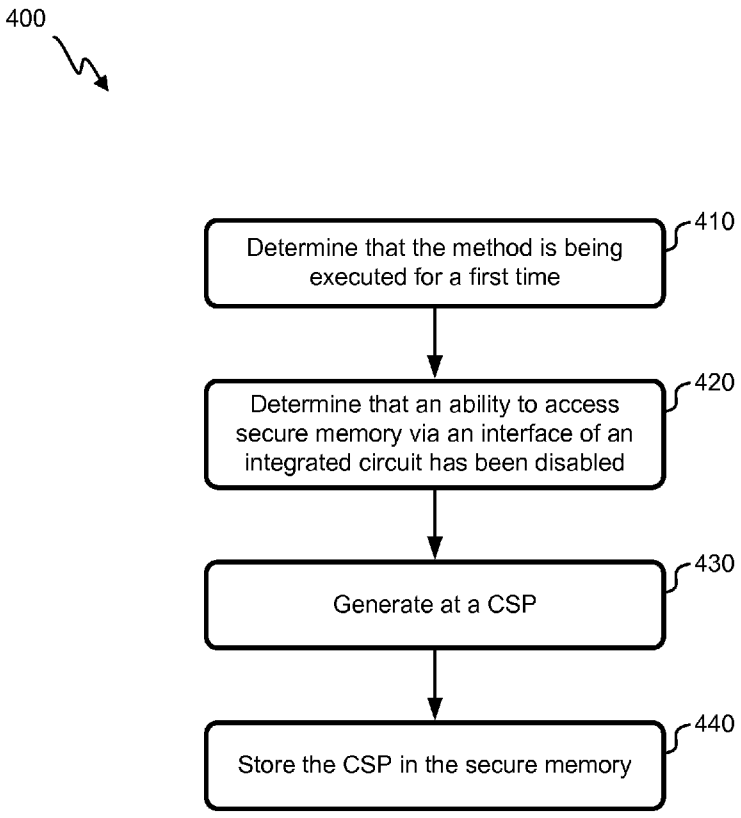
(74) Agents: **MCMILLAN, Scott, L.** et al.; Kilpatrick Townsend & Stockton LLP, 1400 Wewatta Street, Suite 600, Denver, Colorado 80202-5556 (US).

(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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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.

[Continued on next page]

WO 2013/040475 A1

(54) Title: SECURE KEY SELF-GENERATION



(57) Abstract: Techniques are disclosed for providing secure critical security parameter (CSP) generation in an integrated circuit (IC). Embodiments generally include determining that an ability to read the CSP externally (e.g., through a debug interface) has been disabled before the CSP is generated. Depending on the functionality of the device, embodiments can include other steps, such as determining whether software for executing a method for providing a secure CSP is being run for a first time. Among other things, the techniques provided herein for providing secure CSP generation can increase the security of the CSP and reduce manufacturing costs of the IC.

(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, 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, 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))*