

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
12 January 2006 (12.01.2006)

PCT

(10) International Publication Number
WO 2006/004754 A2

(51) International Patent Classification:
G06F 21/00 (2006.01)

(74) Agents: **OGROD, Gregory, D.** et al.; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(21) International Application Number:
PCT/US2005/022937

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(22) International Filing Date: 28 June 2005 (28.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/881,534 29 June 2004 (29.06.2004) US

(71) Applicant (for all designated States except US): **QUALCOMM INCORPORATED** [US/US]; 5775 Morehouse Drive, San Diego, California 92121 (US).

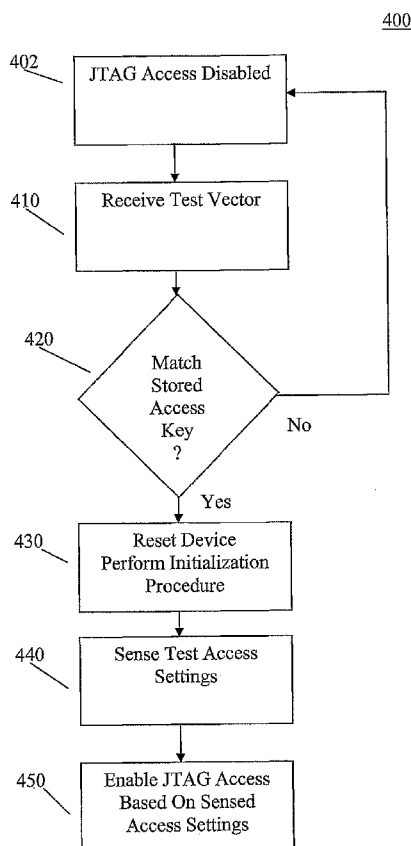
(72) Inventors; and

(75) Inventors/Applicants (for US only): **KITARIEV, Dimitri** [US/US]; 24481 Rue De Gauguin, Laguna Niguel, California 92677 (US). **SHIPPEE, Geoffrey** [US/US]; 2035 Avila Court, La Jolla, California 92037 (US). **VARADARAJAN, Srinivas** [IN/US]; 11491 Trillium Court, San Diego, California 92131 (US).

(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, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: LOCKSTEP MECHANISM TO ENSURE SECURITY IN HARDWARE AT POWER-UP



(57) Abstract: A system and method of ensuring hardware security of a device, such as an integrated circuit having secure data stored thereon. The integrated circuit or other hardware device can implement one or more configurable fuses that limit access to one or more secure locations within the device. The secure locations may contain secure data. The state of the configurable fuses can be ensured, thereby limiting access to secure locations, by forcing the occurrence of a logical state prior to allowing access to hardware locations configured by the fuses. A configurable non-secure access code can be used to force the occurrence of the logical state. Receipt of the non-secure access code by the hardware device forces the occurrence of the hardware state, thereby ensuring access only to those secure locations configured by the fuses.

**Declarations under Rule 4.17:**

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,

GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations

Published:

- without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.