



- (51) **International Patent Classification:**
G06F 21/24 (2006.01) *H03K 19/173* (2006.01)
G06F 9/06 (2006.01)
- (21) **International Application Number:**
PCT/US2012/033911
- (22) **International Filing Date:**
17 April 2012 (17.04.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
13/097,205 29 April 2011 (29.04.2011) US
- (71) **Applicant (for all designated States except US):** ALTERA CORPORATION [US/US]; 101 Innovation Drive - M/S 1405, San Jose, CA 95134-1941 (US).
- (72) **Inventors; and**
- (75) **Inventors/Applicants (for US only):** REESE, Dirk, A. [US/US]; 101 Innovation Drive, San Jose, CA 95134 (US). JOYCE, Juju [US/US]; 101 Innovation Drive, San Jose, CA 95134 (US).
- (74) **Agent:** INGERMAN, Jeffrey, H.; Ropes & Gray LLP, 1211 Avenue Of The Americas, New York, NY 10036 (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, 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.
- (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, 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).

[Continued on next page]

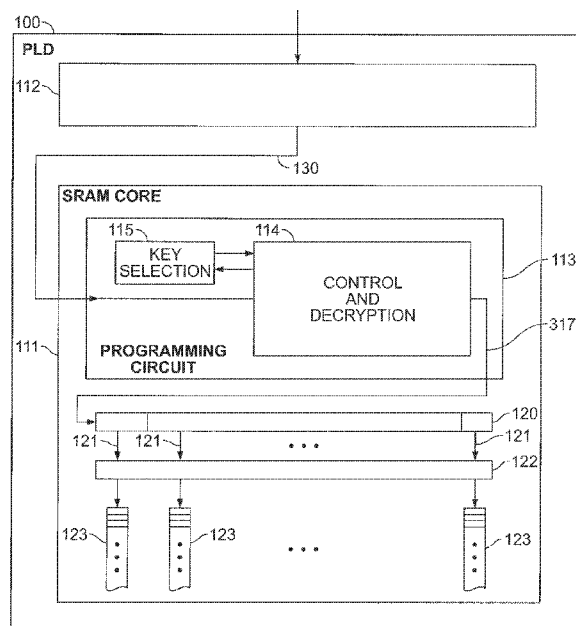
(54) **Title:** METHOD AND APPARATUS FOR SECURING PROGRAMMING DATA OF A PROGRAMMABLE DEVICE

FIG. 1

(57) **Abstract:** Configuration data for a programmable integrated circuit device is at least partially encrypted according to at least one encryption scheme. A plurality of key stores store a plurality of decryption keys for the at least one encryption scheme. Control circuitry identifies a required key from the at least partially encrypted configuration data and generates a key selection signal. Key selection circuitry responsive to the key selection signal reads the plurality of key stores and provides the required key to the control circuitry. The control circuitry may include decryption circuitry that decrypts the at least partially encrypted configuration data using the required key. In some embodiments, different portions of the configuration data, which may represent separate partial reconfigurations of the device, require different decryption keys. Keys may be generated from combinations of the contents of the key stores.

**Published:****(88) Date of publication of the international search report:**

27 December 2012

- *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))*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2012/033911**A. CLASSIFICATION OF SUBJECT MATTER****G06F 21/24(2006.01)i, G06F 9/06(2006.01)i, H03K 19/173(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)

G06F 21/24; G06F 12/14; H04L 9/00; G06F 7/38

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

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: "decryption, circuit, encryption, store, key, configure, selection"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 7058177 B1 (STEPHEN M. TRIMBERGER et al.) 06 June 2006	1-5, 17, 27, 28, 30-32
A	See the abstract, column 7, line 39-column 8, line 19, column 12, line 38-59, column 15, line 15-column 17, line 52 and figure 3.	6-16, 18-26, 29
A	US 2007-0074045 A1 (BRIAN VAN ESSEN et al.) 29 March 2007	1-32
A	See the abstract, paragraph 10, claim 1 and figure 1.	
A	US 2001-0032318 A1 (KUN WAH YIP et al.) 18 October 2001	1-32
A	See the abstract, paragraph 15 and figure 1.	
A	US 6172520 B1 (LAWMAN GARY R. et al.) 09 January 2001	1-32
A	See the abstract, column 8, lines 27-31 and figure 8.	

☐ 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

25 OCTOBER 2012 (25.10.2012)

Date of mailing of the international search report

29 OCTOBER 2012 (29.10.2012)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan
City, 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Soak, Sang Moon

Telephone No. 82-42-481-8470



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2012/033911

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 7058177 B1	06.06.2006	None	
US 2007-0074045 A1	29.03.2007	US 7197647 B1 US 7711964 B2	27.03.2007 04.05.2010
US 2001-0032318 A1	18.10.2001	None	
US 6172520 B1	09.01.2001	None	