PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

9901786-5
1P03

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00

A1

(11) International Publication Number: WO 98/19420

(43) International Publication Date: 7 May 1998 (07.05.98)

(21) International Application Number: PCT/US97/14442

(22) International Filing Date: 15 August 1997 (15.08.97)

(30) Priority Data:
08/735,976 25 October 1996 (25.10.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

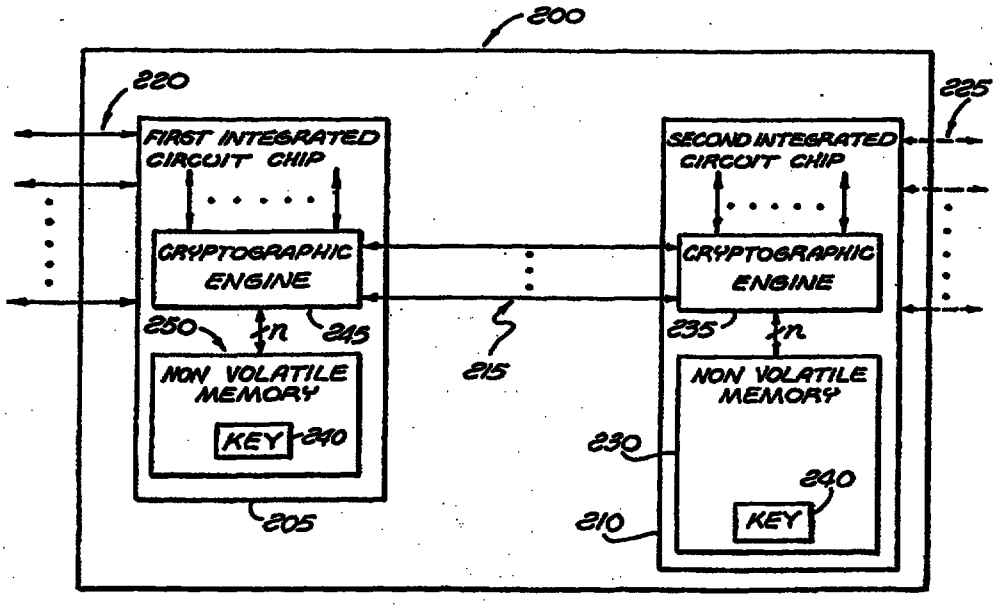
(72) Inventor: DAVIS, Derek, L.; 4509 E. Desert Trumpet Road, Pheonix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(54) Title: A CIRCUIT AND METHOD FOR ENSURING INTERCONNECT SECURITY WITHIN A MULTI-CHIP INTEGRATED CIRCUIT PACKAGE



(57) Abstract

Circuitry implemented within a multi-chip module (200) comprising a first integrated circuit chip (205) and a second integrated circuit chip (210) coupled together through an interconnect (215). Both the first and second integrated circuit chips include a cryptographic engine (245, 235) coupled to the interconnect and a non-volatile memory element (250, 230) used to contain key information (240). These cryptographic engines are solely used to encrypt outgoing information being output across the interconnect or to decrypt incoming information received from the interconnect. This prevents fraudulent physical attack of information transmitted across the interconnect.