9805295-4
IDOS COPY

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: WO 97/39552

(43) International Publication Date: 23 October 1997 (23.10.97)

(21) International Application Number: PCT/US97/04697

(22) International Filing Date: 17 March 1997 (17.03.97)

(30) Priority Data:
08/633,581 17 April 1996 (17.04.96) US

(71) Applicant (*for all designated States except US*): INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventor; and

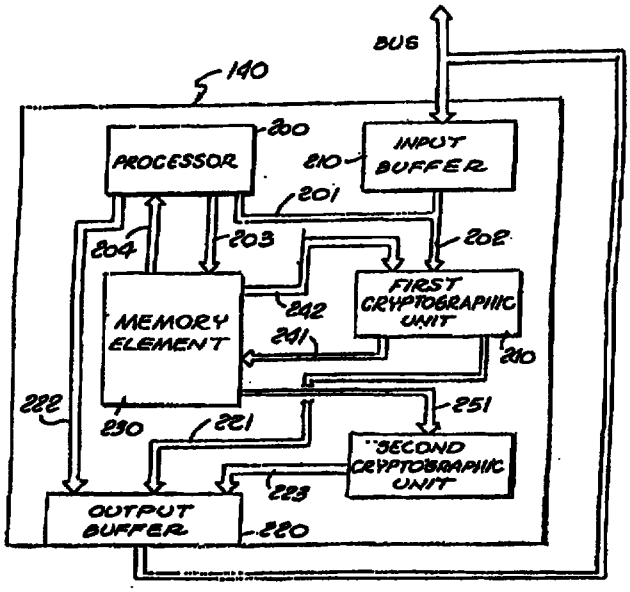
(75) Inventor/Applicant (*for US only*): DAVIS, Derek, L. [US/US]; 4509 E. Desert Trumpet Road, Phoenix, AZ 85044 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman L.L.P., 1279 Oakmead Parkway, Sunnyvale, CA 94086 (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, 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), TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), 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.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: AN APPARATUS AND METHOD FOR RE-ENCRYPTING DATA



(57) Abstract

A cryptographic device (140) formed as an integrated circuit encapsulated in an integrated circuit package. The cryptographic device (140) decrypts information having a first encrypted format (202) that is input into the cryptographic device producing information in a non-encrypted format (241). The information in the non-encrypted format (241) is subsequently re-encrypted into a second encrypted format (223) which is output from the cryptographic device (140). The decryption and re-encryption operations are accomplished entirely within the cryptographic device (140).