

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/32, G06F 12/14	A1	(11) International Publication Number: WO 98/15086
		(43) International Publication Date: 9 April 1998 (09.04.98)
(21) International Application Number: ☒ PCT/US97/13518 (22) International Filing Date: 30 July 1997 (30.07.97) (30) Priority Data: 08/722,298 ☒ 30 September 1996 (30.09.96) ☒ 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, Phoenix, 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, GB, 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.

(54) Title: SECURE BOOT

(57) Abstract

A subsystem prevents unauthorized replacement of boot-up firmware (e.g., BIOS (63)) embedded in modifiable non-volatile memory devices (620) such as flash memory. The firmware device is contained in a secure boot device (54) which is responsive to the host processor (50). The security protection is established by the encryption and decryption of the boot-up instructions using a secret key (64) shared by both the secure boot device (54) and the host processor (50).

