CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04L 9/32

A3

(11) International Publication Number: WO 00/27069

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25293

(22) International Filing Date: 29 October 1999 (29.10.99)

(30) Priority Data:
60/106,267 30 October 1998 (30.10.98) US

(71) Applicant *(for all designated States except US)*: CERTCO INCORPORATED [US/US]; 22nd floor, 55 Broad Street, New York, NY 10004 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: YUNG, Marcel, M. [IL/US]; 605 W. 112th Street, New York, NY 10025 (US). FRANKEL, Yair [US/US]; 122 Harrison, Westfield, NJ 07090 (US).

(74) Agents: HUANG, Stuart, T, F. et al.; Steptoe & Johnson LLP, 1330 Connecticut Avenue, N.W., Washington, DC 20036 (US).

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

Published
With international search report.

(88) Date of publication of the international search report:
27 July 2000 (27.07.00)

(54) Title: INCORPORATING SHARED RANDOMNESS INTO DISTRIBUTED CRYPTOGRAPHY

(57) Abstract

A method of distributed cryptography for high consequence security systems which employs randomness between operating parties. Shared randomness is accomplished by sharing cryptographic keys stored in secure hardware tokens by potentially less secure software or general purpose computing units that perform distributed cryptography. The shared randomness is based on shared keys (at the tokens) and unique context. Shared random values are incorporated into the computation of partial results used in the distributed cryptographic calculation. The incorporation of shared randomness provides a hand–shake among the hardware tokens. When the operation is successful, a result is computed with assurance that the correct parties have taken part in forming the result. The hand–shake assures binding of operating parties and added system security.

*(Referred to in PCT Gazette No. 44/2000, Section II)