(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 February 2007 (22.02.2007)

PCT

(10) International Publication Number
WO 2007/019614 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/AU2006/001159

(22) International Filing Date: 15 August 2006 (15.08.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2005904465 18 August 2005 (18.08.2005) AU

(71) Applicant *(for all designated States except US)*: **ENTROPIC TECHNOLOGIES PTY LTD** [AU/AU]; 28/82 Royal Street, East Perth, Perth, Western Australia 6004 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **ZAHARI, Azman** [MY/MY]; 10 Lorong 5/10 B Section 5, Petaling Jaya, 46000 (MY).

(74) Agent: **HOLLIDAY, Neal, Joseph**; Lord And Company, 4 Douro Place, West Perth, Perth, Western Australia 6005 (AU).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, 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, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD FOR CODE GENERATION

A Code generation parameter	B Personal Identification Code	C Product (A x B)	D Encryption Code (generated from C by MD5 Hash algorithm)
1	78936898	78936898	26ebd4138b1d297caebcedd04bf6750b
2	ditto	157873796	d65841ba44e2b3beb59d06882b199d86
3	ditto	236810694	c61dfc808900d5d29153fa38e25c3c98
4	ditto	315747592	de49e630cddcd8d1f13ce93b18904d3f
5	ditto	394684490	3e5a78f6883328f2043cf76c5d45f307
6	ditto	473621388	31a9611d09a579765403a67f9d554cbc
7	ditto	552558286	dc407eef922a5e8217af18ec7bf8ce8e
8	ditto	631495184	bc0fb4a9672f26ea920a470682cb0021
9	ditto	710432082	2068cd7e14ce3a5629987df23f984267
10	ditto	789368980	6e8207549b709605ad578a4be12efe15
11	ditto	868305878	9aadb0a19bdc0b2943287806dd91e0c2
12	ditto	947242776	8758591d002d0c1f51963d6beccbb4184
13	ditto	1026179674	45a6e573e18d1fb0bbb99c7edcdc4744
14	ditto	1105116572	a3cfefffbc4df36c0e6829ab77f7ecff
15	ditto	1184053470	87915135246e94807c3961ac31d3874a
16	ditto	1262990368	bf31430848b47d10092213ffac5da9f2
17	ditto	1341927266	098bb1971130c22c316433f2c1b7a7e3
18	ditto	1420864164	9550248fb82035f7da9db1dce201c45e
19	ditto	1499801062	95b66f40490fdb5a569fbeadd511a078
20	ditto	1578737960	8eb160b3cc2397097b41cd7ce8b1b85d
21	ditto	1657674858	eb8adb13c179cf9404c3f775eeb3a610
22	ditto	1736611756	5f1a5a6ea784e0f7057e1689a2a3abc7
23	ditto	1815548654	91f504932a27efa17ff9c147e3b5c798
24	ditto	1894485552	703ebb8f3124719aa15ed2ab762b7d84
25	ditto	1973422450	b8f227984183853e4bd77a0e7599254ea
26	ditto	2052359348	b6dc9fb3ab55d845bfaf431491acb5cb
27	ditto	2131296246	264e8c6e89a18e5401867c745ed8de57
28	ditto	2210233144	8e0305de214410579f2b6b69fa4bdec8
29	ditto	2289170042	87a7a858b38d54246ef7476f9308fe27
30	ditto	2368106940	585c47be5f65cdf9cfdcd03268c38b59

(57) Abstract: A method for generating codes for encrypting data of an encrypting device and for decrypting said data by a decrypting device. The method includes the steps of providing a personal identification code to the encrypting device, the personal identification code being known or obtainable by the decrypting device, and selecting from a set of code generation parameters a current code generation parameter. The encryption code for encrypting the data of the encrypting device is generated by an algorithm, the algorithm being a function of the current code generation parameter and the personal identification code. The current code generation parameter is either known to the decrypting device based on its position in the sequence of said code generation parameters, or is transmitted to the decrypting device such that the decrypting device can generate the encryption code using the current code generation parameter, the personal identification code and the algorithm to allow decryption of the data.

WO 2007/019614 A1