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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 December 2005 (08.12.2005)

PCT

(10) International Publication Number
WO 2005/117335 A1

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

(21) International Application Number:
PCT/GB2005/050011

(22) International Filing Date: 4 February 2005 (04.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0411777.6 26 May 2004 (26.05.2004) GB

(71) Applicant *(for all designated States except US)*: **CRYPTOMATHIC LTD** [GB/GB]; 329 Cambridge Science Park, Milton Road, Cambridge, Cambridgeshire CB4 0WG (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **TULIANI, Jonathan, Roshan** [GB/GB]; 206 The Rowans, Milton, Cambridge, Cambridgeshire CB4 6ZL (GB). **LANDROCK, Peter** [DK/DK]; Klostergade 28, 1, DK-8000 Aarhus C (DK).

(74) Agent: **Marks & Clerk**; 66-68 Hills Road, Cambridge, Cambridgeshire CB2 1LA (GB).

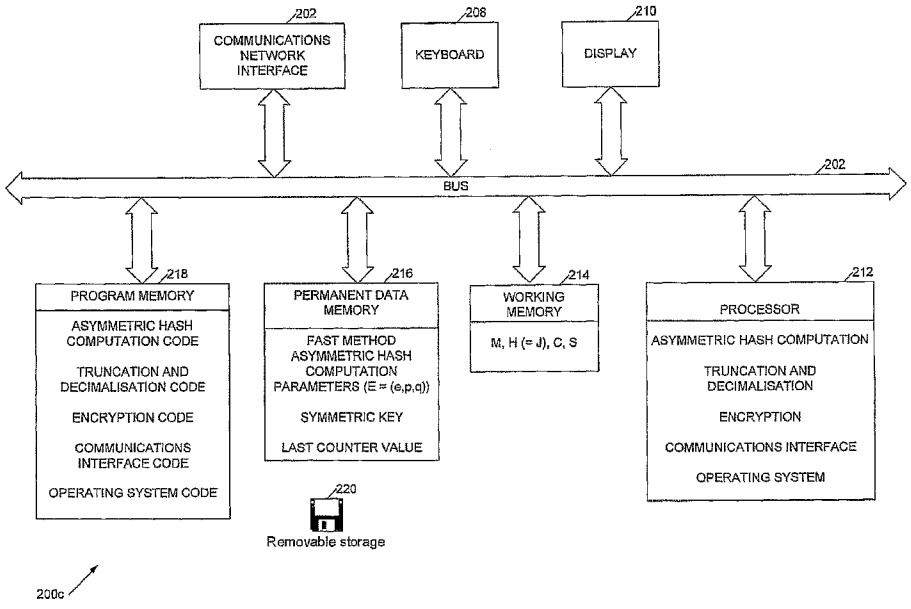
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, 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*

[Continued on next page]

(54) Title: COMPUTATIONALLY ASYMMETRIC CRYPTOGRAPHIC SYSTEMS



(57) Abstract: This invention is generally concerned with methods, apparatus and computer program code for a computationally asymmetric hash function, in particular for use with symmetric cryptographic algorithms. A method of determining a computationally asymmetric hash function value, the method comprising: receiving input data to be hashed; computing an asymmetric value from said input data, said asymmetric value being computable by two methods, a first method employing at least one first parameter and a second method employing at least one second parameter, computation of said asymmetric value by said second method being faster than by said first method; and determining a computationally asymmetric has function value using said asymmetric value.

WO 2005/117335 A1

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.