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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 April 2003 (10.04.2003)

PCT

(10) International Publication Number
WO 03/030442 A3

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US02/31278

(22) International Filing Date: 1 October 2002 (01.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/326,250 1 October 2001 (01.10.2001) US

(71) Applicant *(for all designated States except US)*: **LAYER N NETWORKS, INC.** [US/US]; Patents, 12401 Research Blvd., Building Two, Suite 275, Austin, TX 78759 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **BLAKLEY, George** [US/US]; LAYER N NETWORKS, INC., Patents, 12401 Research Blvd., Building Two, Suite 275, Austin, TX 78759 (US). **DATTA, Rajat** [US/US]; LAYER N NETWORKS, INC., Patents, 12401 Research Blvd., Building Two, Suite 275, Austin, TX 78759 (US). **MITCHELL, Oscar** [US/US]; LAYER N NETWORKS, INC., Patents, 12401 Research Blvd., Building Two, Suite 275, Austin, TX 78759 (US). **STEIN, Kyle** [US/US]; LAYER N NETWORKS, INC., Patents, 12401 Research Blvd., Building Two, Suite 275, Austin, TX 78759 (US).

(74) Agent: **WEISS, Aaron**; THOMPSON & KNIGHT LLP, IP DOCKETING, 98 San Jacinto Blvd., #1200, Austin, TX 78701-4081 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, 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, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
11 December 2003

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.

WO 03/030442 A3

(54) Title: CISPONENTIATION METHOD, SOFTWARE, AND DEVICE FOR EXPONENTIATION

(57) Abstract: A method, software, and device for encrypting data, exchanging keys, and processing data that includes exponentiating by iteratively cisponentiating according to cisponentiator $C(G, E, B, R, m) = G^E BR \bmod m$, wherein G is a fleeting multiplicand base, E is an enduring cisponent, B is a recurring multiplier, R is an enduring factor, and m is a persistent modulus. E may be a fixed characteristic of the cisponentiator. E may also be a power of 2. R may be fixed. In one of many possible combinations, E is a fixed characteristic of the cisponentiator, while R is fixed. In that case also, E may be a power of 2. Modulus m may be fixed. In one of many possible combinations, E is a fixed characteristic of the cisponentiator, R is fixed, and m is fixed. As one of many alternatives, data may be encrypted using asymmetric encryption.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/31278

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 380/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
East

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- A	US 5,046,094 A (KAWAMURA et al) 03 September 1991 (03.09.91) Col. 1, line 40 - Col. 7, line 50 Col. 19, lines 35- 44 Col. 27, lines 22-30	1, 11, 19, 21, 23, 33, 41 --- 2-10, 12-18, 22, 24-32, 34-40, 42, 43
X --- A	US 5,289,397 A (CLARK et al) 22 February 1994 (22.02.94) Col. 1, line 6 - Col. 3, line 6 Col. 4, line 54 - Col. 12, line 55	1, 11, 19, 21, 23, 33, 41 --- 2-10, 12-18, 22, 24-32, 34-40, 42, 43
A	US 6,185,596 B1 (HADAD et al) 06 February 2001 (06.02.01) Col. 1, lines 23 - Col. 9, line 25	1-43
A	US 5,101,431 A (EVEN et al) 31 March 1992 (31.03.92) Col. 1, line 12 - Col. 3, line 7	1-43
A	US 5,321,752 A (IWAMURA et al) 14 June 1994 (14.06.94) Col. 3, line 37 - Col. 7, line 7	1-43

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
25 February 2003 (25.02.2003)

Date of mailing of the international search report
14 MAR 2003

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703)305-3230

Authorized officer
Gilberto Barron
Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

PCT/US02/31278

INTERNATIONAL SEARCH REPORT

C. (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,448,639 A (ARAZI et al) 05 September 1995 (05.09.95) Fig. 1 Col. 1, line 47 - Col. 2, line 15	1-43
A	US 5,513,133 A (CRESSEL et al) 30 April 1996 (30.04.96) Col. 3, lines 15 - Col. 9, line 15	1-43