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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 September 2004 (10.09.2004)

PCT

(10) International Publication Number
WO 2004/077248 A3

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

(21) International Application Number:
PCT/US2004/005125

(22) International Filing Date: 20 February 2004 (20.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/377,346 27 February 2003 (27.02.2003) US

(71) Applicant *(for all designated States except US)*: **REAL-NETWORKS, INC.** [US/US]; 2601 Elliott Avenue, Suite 1000, Seattle, WA 98121 (US).

(72) Inventor: **FU, Xiaodong**; 10746 Main St. #302, Fairfax, VA 22030 (US).

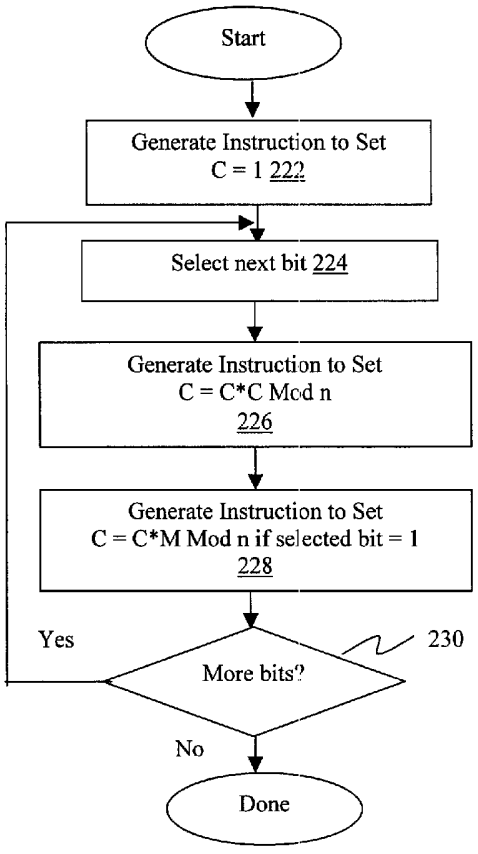
(74) Agents: **KLINDTWORTH, Jason, K.** et al.; Schwabe, Williamson & Wyatt, P.C., Pacwest Center, Suites 1600-1900, 1211 SW Fifth Avenue, Portland, OR 97204 (US).

(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, 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, 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, IT, LU, MC, NL, PT, RO, SE, SI, SK,

[Continued on next page]

(54) Title: KEY BASED DECIPHER INCLUDING ITS GENERATION, DISTRIBUTION AND USAGE



(57) Abstract: A decipher key based decipher with at least a portion of the decipher key dissolved into the decipher is disclosed. The decipher includes in-line instructions specifically designed to incrementally contribute to computation of M^e Mod n, where e is a predetermined at least partially unique decipher key. In one embodiment, the decipher includes a first in-line instruction to set an output variable to equal to 1, and a second in-line instruction to set the output variable to equal to the square of the output variable modulus n. In another embodiment, the decipher includes in-line instructions that perform the incremental computation in accordance with an addition chain of e.

WO 2004/077248 A3

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
3 February 2005

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.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/05125

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 380/030

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. : 380/030 713/151;380/29

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0159589 A1 (She et al.) 31 October 2002, see entire document.	1-51
Y	US 4,405,829 A (Rivest et al.) 20 September 1983, see entire document.	1-51
Y	US 5,535,276 A (Ganesan) 09 July 1996, see entire document.	2-10,12-19,21-27 & 29-51
Y	Koblitz, Neal (A Course in Number Theory and cryptography) Second Edition, 1994.	2-10,12-19,21-27,29-35,37-43,45-51
Y	RSA (A method for Obtaining Digital Signatures and Public-Key Cryptosystems) 1998.	4-10,14-19,23-27,30-35,38-43,46-51
Y,P	US 2004/0005054 A1 (Montgomery et al.) 08 January 2004, see entire document.	8-10,18-19,26-27,34-35,42-43, 50-51

☐ 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	Date of mailing of the international search report
21 July 2004 (21.07.2004)	22 DEC 2004
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer VINCENT TRANS Telephone No. (571) 272-3613

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

Continuation of B. FIELDS SEARCHED Item 3:
USPAT;US-PGPUB;EPO;JPO;DERWENT;IBM_TDB
key,based,wireless,phone,cellphone,variables,conditional,chaining,near,method,cryptography,addition,decipher,part