

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
6 February 2003 (06.02.2003)

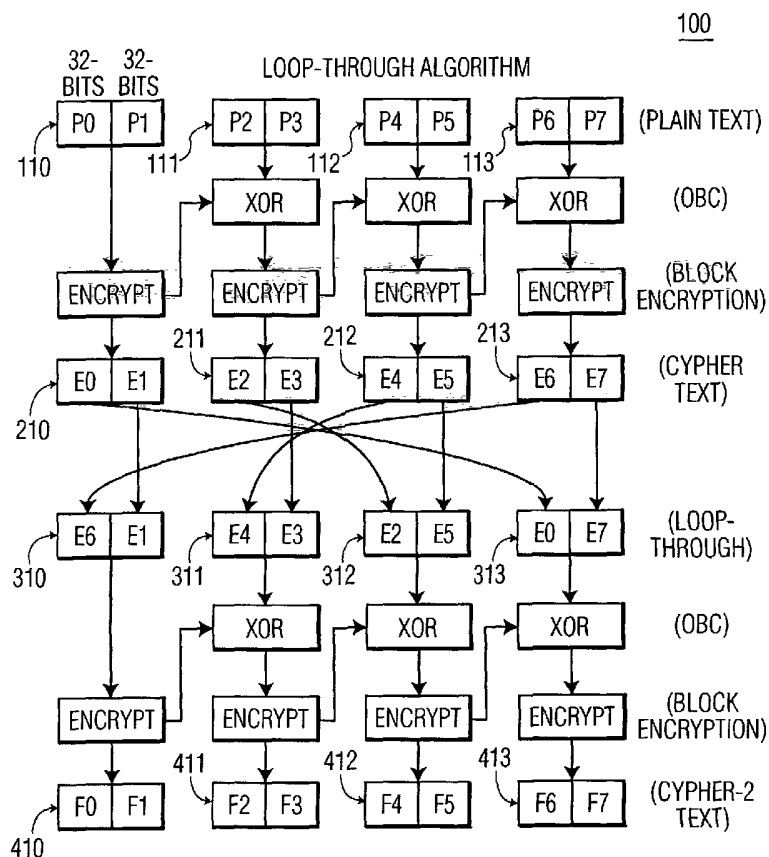
PCT

(10) International Publication Number
WO 03/010916 A3

- (51) International Patent Classification⁷: **H04L 9/00** (74) Agents: **TRIPOLI, Joseph, S.** et al.; Thomson multimedia Licensing Inc., P.O. Box 5312, Princeton, NJ 08540 (US).
- (21) International Application Number: PCT/US02/10691
- (22) International Filing Date: 3 April 2002 (03.04.2002) (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, VN, YU, ZA, ZM, ZW.
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 60/282,056 7 April 2001 (07.04.2001) US
- (71) Applicant (*for all designated States except US*): **THOMSON LICENSING S.A.** [FR/FR]; 46, Quai A. Le Gallo, F-92648 Boulogne Cedex (FR).
- (72) Inventor; and
- (75) Inventor/Applicant (*for US only*): **RHOADS, Steven, C.** [US/US]; 140 Parkview Road, Carmel, IN 46032 (US).
- (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, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR ENCRYPTING CONTENT



(57) Abstract: A method for encrypting content, said method comprising encrypting a first plurality of separate blocks of content to obtain a second plurality of blocks of once-encrypted content, exchanging at least a portion of the content stored in a first set of blocks of the second plurality of blocks of once-encrypted content with at least a portion of the content stored in a second set of blocks of the second plurality of blocks of once-encrypted content to generate a third plurality of blocks of once-encrypted content, and encrypting the third plurality of blocks of encrypted content to generate a fourth plurality of blocks of twice-encrypted content.



WO 03/010916 A3



Published:

— *with international search report*

(88) Date of publication of the international search report:

2 October 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.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/10691

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/00

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)
IPC 7 H04L

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 practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 384 478 A (ANT NACHRICHTENTECH) 29 August 1990 (1990-08-29) abstract column 1, line 1 -column 2, line 15 ---	1-19
Y	GIDDY J P ET AL: "AUTOMATED CRYPTANALYSIS OF TRANSPOSITION CIPHERS" COMPUTER JOURNAL, OXFORD UNIVERSITY PRESS, SURREY, GB, vol. 37, no. 5, 1994, pages 429-436, XP000485457 ISSN: 0010-4620 page 429, left-hand column page 430, right-hand column --- -/--	1-19



Further documents are listed in the continuation of box C.



Patent family members are listed in 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 document but 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.
- *G* document member of the same patent family

Date of the actual completion of the international search

13 June 2002

Date of mailing of the international search report

08/07/2002

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 02/10691

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIER B: "Applied cryptography, second edition" JOHN WILEY & SONS, 1996, pages 367-368, XP002202114 NEW YORK, US ISBN: 0-471-11709-9 page 367 -page 368 -----	1-19

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/US 02/10691

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
EP 0384478	A	29-08-1990	DE	3905667 A1	30-08-1990
			EP	0384478 A2	29-08-1990