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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 August 2002 (01.08.2002)

PCT

(10) International Publication Number
WO 02/060116 A3

(51) International Patent Classification[7]: H04L 9/08, 29/06

(21) International Application Number: PCT/GB02/00305

(22) International Filing Date: 23 January 2002 (23.01.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/770,877 26 January 2001 (26.01.2001) US

(71) Applicant: INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) Applicant (for MG only): IBM UNITED KINGDOM LIMITED [GB/GB]; PO Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

(72) Inventors: LOTSPIECH, Jeffrey, Bruce; 982 Foothill Drive, San Jose, CA 95123 (US). NAOR, Dalit; 247 Fulton Street, Palo Alto, CA 94301 (US). NAOR, Simeon; 247 Fulton Street, Palo Alto, CA 94301 (US).

(74) Agent: BURT, Roger, James; IBM United Kingdom Limited, Intellectual Property Law, Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(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, UZ, 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, 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).

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:
26 September 2002

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 02/060116 A3

(54) Title: METHOD FOR BROADCAST ENCRYPTION

(57) Abstract: A tree is used to partition stateless receivers in a broadcast content encryption system into subsets. Two different methods of partitioning are disclosed. When a set of revoked receivers is identified, the revoked receivers define a relatively small cover of the non-revoked receivers by disjoint subsets. Subset keys associated with the subsets are then used to encrypt a session key that in turn is used to encrypt the broadcast content. Only non-revoked receivers can decrypt the session key and, hence, the content.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/GB 02/00305

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 641 103 A (ALGORITHMIC RES LTD) 1 March 1995 (1995-03-01) page 3, line 17 -page 3, line 24 page 3, line 33 -page 3, line 35 page 4, line 57 -page 5, line 1 ---	1-13
A	ABDALLA M ET AL: "KEY MANAGEMENT FOR RESTRICTED MULTICAST USING BROADCAST ENCRYPTION" , IEEE / ACM TRANSACTIONS ON NETWORKING, IEEE INC. NEW YORK, US, VOL. 8, NR. 4, PAGE(S) 443-454 XP000959120 ISSN: 1063-6692 page 445, left-hand column, line 49 -page 445, right-hand column, line 37 page 448, left-hand column, line 33 -page 451, left-hand column, line 23 --- -/--	1-13

[X] Further documents are listed in the continuation of box C.

[X] 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.

'&' document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 July 2002	26/07/2002

Name and mailing address of the ISA	Authorized officer
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	Apostolescu, R

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	CHOR B ET AL: "Tracing traitors" , ADVANCES IN CRYPTOLOGY (CRYPTO). SANTA BARBARA, AUG. 21 - 25, 1994, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, VOL. CONF. 14, PAGE(S) 257-270 XP002097845 ISBN: 3-540-58333-5 page 258, line 6 -page 258, line 9 page 258, line 20 -page 258, line 21 page 259, line 36 -page 260, line 13 ---	1,13
A	BLUNDO C ET AL: "TRADE-OFFS BETWEEN COMMUNICATION AND STORAGE IN UNCONDITIONALLY SECURE SCHEMES FOR BROADCAST ENCRYPTION AND INTERACTIVE KEY DISTRIBUTION" , ADVANCES IN CRYPTOLOGY - CRYPTO '96. 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, VOL. CONF. 16, PAGE(S XP000626596 ISBN: 3-540-61512-1 page 389, line 16 -page 389, line 46 -----	1,13

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/GB 02/00305

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0641103 A	01-03-1995	IL 106796 A	20-11-1997
		EP 0641103 A2	01-03-1995
		US 5592552 A	07-01-1997