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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2004 (05.02.2004)

PCT

(10) International Publication Number
WO 2004/012384 A3

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

(21) International Application Number:
PCT/US2003/023473

(22) International Filing Date: 25 July 2003 (25.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/399,092 27 July 2002 (27.07.2002) US

(71) Applicant and
(72) Inventor: **HOTZ, Jimmy, Christian** [US/US]; 3094 Fort Courage Avenue, Thousand Oaks, CA 91360 (US).

(74) Agents: **RITCHIE, David, B.** et al.; THELEN REID & PRIEST LLP, P.O. BOX 640640, San Jose, CA 95164-0640 (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, 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 *(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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

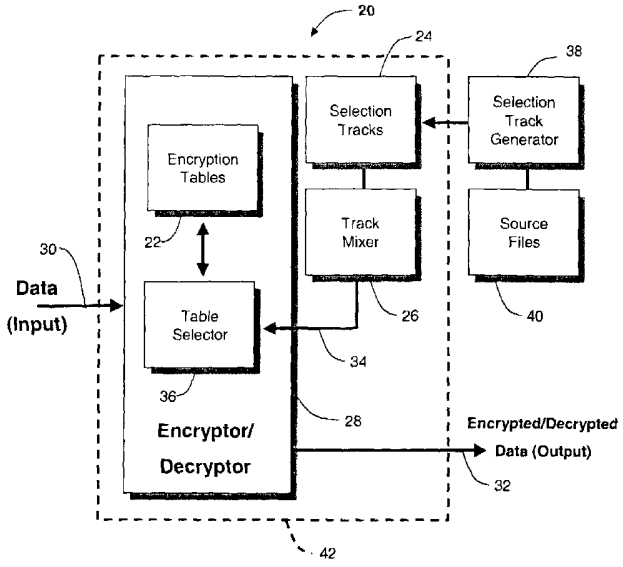
Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

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:
18 November 2004

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.

(54) Title: APPARATUS AND METHOD FOR ENCTYPTION AND DECRYPTION



(57) Abstract: An apparatus and method for encrypting/decrypting data include (a) a first plurality of encryption tables, each of the encryption tables being capable of transforming a data value into an encrypted/decrypted value, the data value corresponding to a unit of the data, the encrypted/decrypted value corresponding to a unit of encrypted/decrypted data, (b) a second plurality of selection tracks, each of the selection tracks including a series of values having a certain pattern, (c) a track mixer coupled to the second plurality of selection tracks, adapted to combine corresponding values of the selection tracks to produce a series of combined values, and (d) an encryption/decryption module coupled to the first plurality of encryption tables and the track mixer, adapted to transform each unit of the data into a unit of encrypted/decrypted data using an encryption table selected for that unit according to a combined value in the series of combined values.

WO 2004/012384 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/23473

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/06

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, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 4 853 962 A (BROCKMAN ROBERT T) 1 August 1989 (1989-08-01)	1-10, 17-20, 25, 29-32, 34-41, 65,68-72
Y	abstract column 1, line 61 - column 5, line 39 figures 3-7,9,10	11

X	US 5 414 771 A (FAWCETT JR KENNETH J) 9 May 1995 (1995-05-09)	68-75
A	abstract column 4, line 4 - column 11, line 45; figures 1,2	2,18-20, 25-28, 30-32

	-/--	

[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
1 June 2004	16. 09. 2004

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	Dujardin, C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/23473

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 003 596 A (WOOD MICHAEL C) 26 March 1991 (1991-03-26)	11
A	abstract column 7, line 1 - column 15, line 57; figures 2,3,8-11	1,10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 03/23473

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-48, 65, 68-75

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-48,65,68-75

Apparatus, method and program storage device for encrypting/decrypting data using a plurality of encryption tables, a plurality of selection tracks, a track mixer and an encryption/decryption module. Pseudo-random generator comprising a selection track generator and a track mixer.

---

2. claims: 49-59,60-64,66-67

Apparatus, method and program storage device for automatic set up of an encryptor/decryptor on an apparatus or for the authentication of an apparatus, wherein the apparatus has an identification code unique to the apparatus and a setup file associated with the identification code.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 03/23473

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 4853962	A	01-08-1989	NONE		
US 5414771	A	09-05-1995	NONE		
US 5003596	A	26-03-1991	AT	160476 T	15-12-1997
			AU	635466 B2	18-03-1993
			AU	6043190 A	03-04-1991
			CA	2064769 A1	18-02-1991
			DE	69031736 D1	02-01-1998
			DE	69031736 T2	04-06-1998
			EP	0489742 A1	17-06-1992
			JP	5501925 T	08-04-1993
			JP	3188940 B2	16-07-2001
			WO	9103113 A1	07-03-1991