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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 January 2007 (25.01.2007)

PCT

(10) International Publication Number
WO 2007/011990 A3

(51) International Patent Classification:
H04L 9/32 (2006.01) *H04L 9/30* (2006.01)

(21) International Application Number:
PCT/US2006/027978

(22) International Filing Date: 17 July 2006 (17.07.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/182,520 15 July 2005 (15.07.2005) US

(71) Applicant *(for all designated States except US)*: **TYFONE INC.** [US/US]; 5520 SW Macadam Ave., Suite 250, Portland, OR 97219 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NARENDRA, Siva G.** [IN/US]; 7180 SW, 84th Ave, Portland, OR 97223 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore, Karnataka 560 066 (IN). **SPITZER, Thomas N.** [US/US]; 2642 SW, Bucharest Ct., Portland, OR 97225 (US).

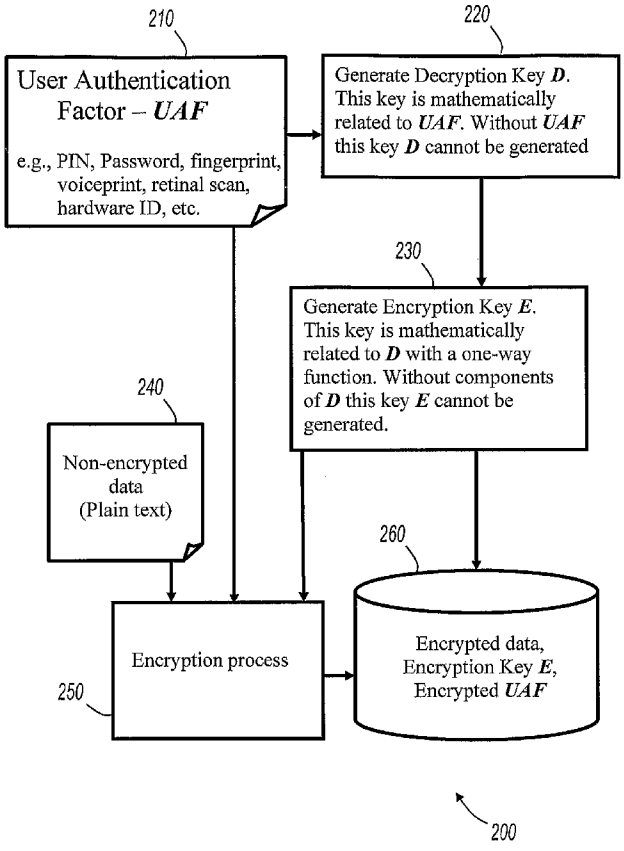
(74) Agent: **LEMOINE PATENT SERVICES**; Intellevate LLC-Patent & Trademark Services, 900 Second Ave South, Suite 1700, Minneapolis, MN 55402 (US).

(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, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, 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, IS, IT, LT, LU, LV, MC, NL, PL, PT,

[Continued on next page]

(54) Title: ASYMMETRIC CRYPTOGRAPHY WITH USER AUTHENTICATION



(57) Abstract: A device uses a user authentication factor to generate a decryption key for use in asymmetric cryptography. An encryption key is generated from the decryption key using a one-way function.

WO 2007/011990 A3

RO, SE, SI, SK, 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:
27 September 2007

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/US2006/027978

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/32 H04L9/30

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)
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, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	ULUDAG U ET AL: "Multimedia content protection via biometrics-based encryption" MULTIMEDIA AND EXPO, 2003. PROCEEDINGS. 2003 INTERNATIONAL CONFERENCE ON 6-9 JULY 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 6 July 2003 (2003-07-06), pages 237-240, XP010650396 ISBN: 0-7803-7965-9 the whole document	1-41
Y	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997, CC PRESS LLC , USA , XP002442440 page 330 - page 331 page 386 - page 389 page 394 - page 395 page 551 - page 553	1-41

-/--

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

[X] 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 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
18 July 2007	01/08/2007

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	SAN MILLAN MAESO, J

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/027978

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 00/36566 A (KONINKL PHILIPS ELECTRONICS NV [NL]) 22 June 2000 (2000-06-22) abstract figures 3,4 page 2, line 29 - page 3, line 16	1-41

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/027978

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0036566 A	22-06-2000	CN 1297553 A	30-05-2001
		EP 1057145 A1	06-12-2000
		JP 2002532997 T	02-10-2002
		TW 472217 B	11-01-2002
		US 2002124176 A1	05-09-2002