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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
11 October 2007 (11.10.2007)

PCT

(10) International Publication Number
WO 2007/113796 A3

(51) International Patent Classification:
H04L 9/00 (2006.01) *H04K 1/06* (2006.01)

(21) International Application Number:
PCT/IL2007/000364

(22) International Filing Date: 20 March 2007 (20.03.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
174784 4 April 2006 (04.04.2006) IL

(71) Applicant *(for all designated States except US)*: **NDS LIMITED** [GB/GB]; One Heathrow Boulevard, 286 Bath Road, West Drayton Middlesex UB7 0DQ (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MANTIN, Itsik** [IL/IL]; 6 Hamizpe Street, 73142 Shoham (IL). **GRABOVSKY, Aharon** [IL/IL]; 71937 Moshav Nerya (IL).

(74) Agents: **SANFORD T. COLB & CO.** et al.; P.O. Box 2273, 76122 Rehovot (IL).

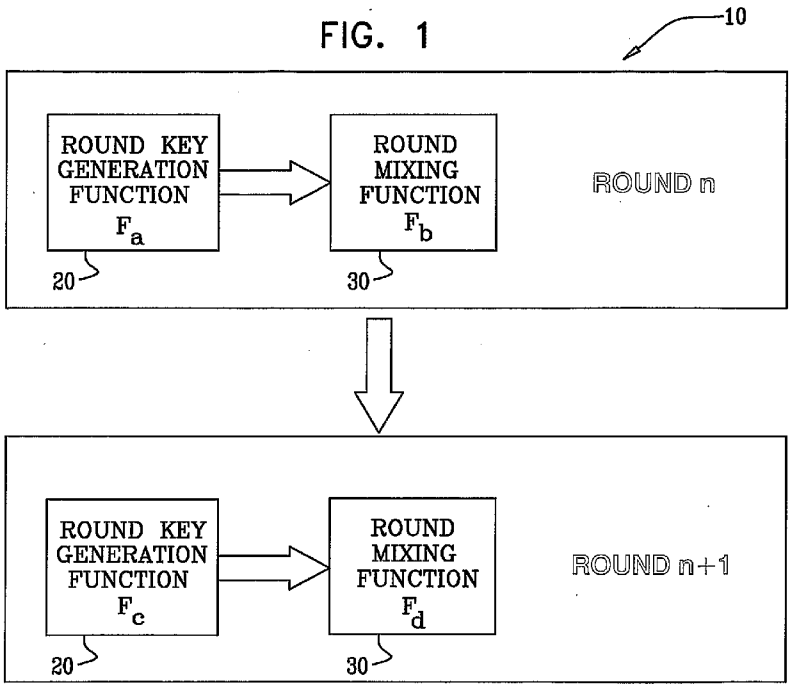
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, 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, MT, NL, PL, PT, 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*

(88) Date of publication of the international search report:
9 April 2009

(54) Title: ROBUST CIPHER DESIGN



(57) Abstract: In an iterated block cipher, a method for round key encryption and key generation, the method including providing a first function Fi and a second function Fj, providing a round key generation function, the round key generation function being operative to utilize, in any given round, exactly one of the first function Fi, and the second function Fj, providing a round mixing function, the round mixing function being operative to utilize, in any given round, exactly one of the first function Fi, and the second function Fj, utilizing the round key generation function in at least a first round to generate a second round key for use in a second round, and utilizing the round mixing function in at least the first round to mix a first round key with a cipher state, wherein one of the following is performed in the first round the round key generation function utilizes the first function Fi to generate the second round key for use in the second round, substantially simultaneously with the round key mixing function utilizing the second function Fj to mix the first round key with the cipher state, and the round key generation function utilizes the second function Fj to generate the second round key for use in the second round, substantially simultaneously with the round key mixing function utilizing the first function Fi to mix the first round key with the cipher state. Related apparatus and methods are also described.

WO 2007/113796 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL07/00364

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **H04L 9/00**(2006.01);**H04K 1/06**(2006.01)

USPC: 380/37
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. : 380/37

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)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/0047466 A1 (FELDMAN et al.) 11/November 2004 (11.11.2004), Entire Document.	1-47
A	US 2003/0108195 A1 (OKADA) 12 June 2003 (12.06.2003), Entire Document	1-47
A	US 2006/0029223 A1 (ARI) 09 February 2006 (09.02.2006), Entire Document.	1-47
A	Schneier, B., Applied Cryptograph, Protocols, Algorithms, and Source Code in C., Second Edition, 1996, pages 351-353.	1-47

☐ 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
14 March 2008 (14.03.2008)	28 MAR 2008
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. (571) 273-3201	Authorized officer /Tongoc Tran/ Telephone No. (571) 272-3843