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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2006 (26.10.2006)

PCT

(10) International Publication Number
WO 2006/113541 A3

(51) International Patent Classification:
H04L 9/00 (2006.01)

(21) International Application Number:
PCT/US2006/014258

(22) International Filing Date: 13 April 2006 (13.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/670,934 13 April 2005 (13.04.2005) US

(71) Applicant *(for all designated States except US)*: **NORTHWESTERN UNIVERSITY** [US/US]; 633 Clark Street, Evanston, Illinois 60208 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LIANG, Chuang** [CN/US]; 800 Hinman Avenue #714, Evanston Illinois 60202 (US). **KANTER, Gregory** [US/US]; 320 West Illinois Street, #1117, Chicago, Illinois 60610 (US). **CORNDORF, Eric** [US/US]; 720 W. Lake Street #408, Minneapolis, Minnesota 55408 (US). **KUMAR, Prem** [US/US]; 7727 N. Kildare Avenue, Skokie, Illinois 60076-3605 (US).

(74) Agents: **KALINOWSKI, Leonard, J.** et al.; REINHART BOERNER VAN DEUREN S.C, 1000 N. Water St., Suite 2100, Milwaukee, Wisconsin 53202 (US).

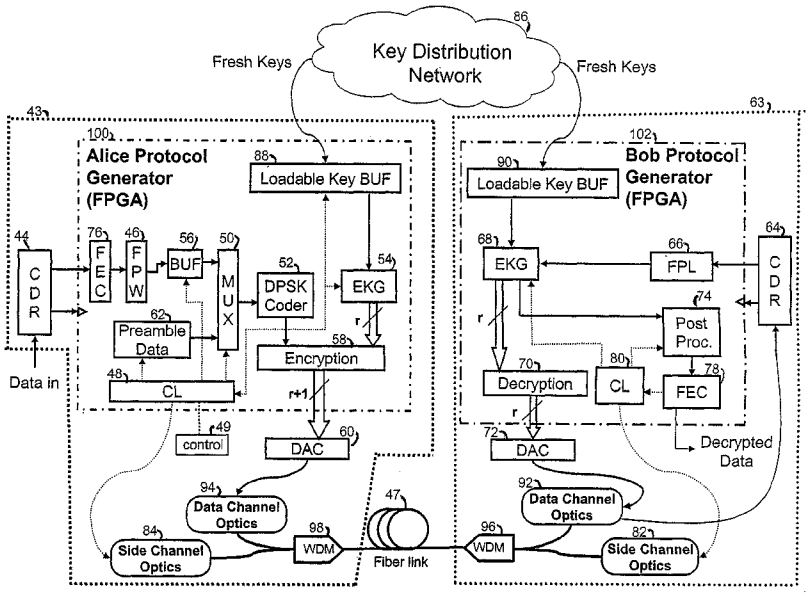
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, 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, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, 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, 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*

[Continued on next page]

(54) Title: STREAMING IMPLEMENTATION OF ALPHAETA PHYSICAL LAYER ENCRYPTION



(57) Abstract: A method of synchronizing the encryption/ decryption functions of an AlphaEta physical-layer encryption or key generation system. The method includes the insertion of a header to indicate the start of encryption after clock-synchronization has been established. The method also allows for a side- channel to signal other useful information, such as a loss-of -synchronization signal from Bob or to synchronize a dynamic key change.

WO 2006/113541 A3

— *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:
22 November 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/US 06/14258

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8): H04L 009/00 (2007.01)
USPC: 713/151; 380/28
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(8): H04L 009/00 (2007.01)
USPC: 713/151; 380/28

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC: 713/151; 380/28; 725/143; 725/144; 725/148; 725/151

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST (PGPB,USPT,EPAB,JPAB); DialogPRO(Engineering); Google Scholar; Search terms: synchronize, encrypt, decrypt, physical layer, key generate, insert, clock, side channel, signal, loss, dynamic, stream

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2005/0060759 A1 (Rowe et al.) 17 March 2005 (17.03.2005), entire document especially Abstract, para [0313], para [0016], para [0144], para [0149] and FIG.7.	1-24
A	CATTANEO, G. et al. 'The Design and Implementation of a Transparent Cryptographic Filesystem for UNIX'. In Proceedings of the Annual USENIX Technical Conference, FREENIX Track, pages 245-252, June 2001. [retrieved 09 June 2007] - Retrieved from the Internet: <URL: http://www.usenix.org/publications/library/proceedings/usenix01/freenix01/full_papers/cattaneo/cattaneo.pdf >	1-24
A	KIM. Y.C. et al. 'Architecture and Implementation of an Encryption Processor Suitable for a Noisy Channel'. In South Korea Conference: Proceedings of the International Conference on Communications in Computing. CIC'2000 , Page: 129-34, and in Proceedings of CIC 2000 International Conference on Communicating in Computing , Sponsor: Buchtel College of Arts & Sci., Univ. Akron , 26-29 June 2000 , Las Vegas, NV, USA [retrieved 09 June 2007] - Retrieved from the Internet: <URL: http://altair.chonnam.ac.kr/~ngi/seminar/mpls/paper3.doc	1-24

☐ Further documents are listed in the continuation of Box C. ☐

* 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 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
09 June 2007 (09.06.2007)	25 SEP 2007
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: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (April 2005)