

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 May 2006 (04.05.2006)

PCT

(10) International Publication Number
WO 2006/047134 A3

(51) International Patent Classification:
H04L 9/08 (2006.01)

(74) Agent: **GORTYCH, Joseph, E.**; Opticus IP, 7791 Alister Mackenzie Drive, Sarasota, FL 34240 (US).

(21) International Application Number:
PCT/US2005/037352

(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, 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.

(22) International Filing Date: 18 October 2005 (18.10.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/970,043 21 October 2004 (21.10.2004) US

(71) Applicant (*for all designated States except US*): **MAGIQ TECHNOLOGIES, INC.** [US/US]; 171 Madison Avenue, Suite 1300, New York, NY 10016 (US).

(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).

(72) Inventors; and

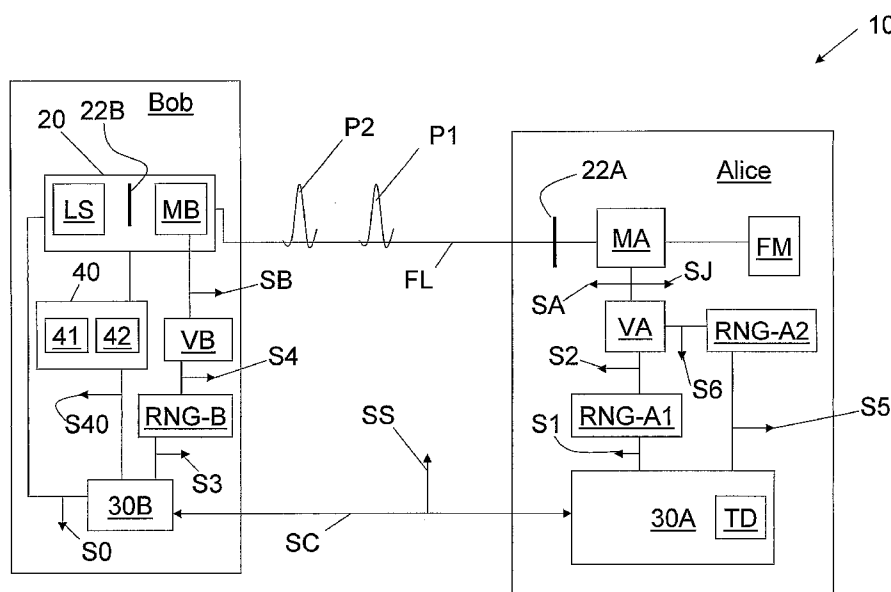
(75) Inventors/Applicants (*for US only*): **VIG, Harry** [CA/US]; 8 Kohlrausch Avenue, North Billerica, MA 01862 (US). **YOUNG, Jonathan** [US/US]; 145 State Street, Newburyport, MA 01950 (US). **TRIFONOV, Alexei** [US/US]; 69 Park Drive, Apt. 8, Boston, MA 02251 (US). **MITCHELL, J. Howell, Jr.** [US/US]; 324 Boston Post Road, Amherst, NH 03031 (US).

Published:

— with international search report

[Continued on next page]

(54) Title: CONSTANT MODULATION FOR ENHANCED QKD SECURITY



(57) Abstract: A method of improving the security of a QKD system (10) is disclosed. The method includes randomly modulating a modulator (MA) in a QKD station (Alice) both within the gating interval (GI) with a control signal (SA) and outside of the gating interval with a jabber signal (SJ), while recording those modulations made during the gating interval. Such continuous modulation prevents an eavesdropper from assuming that the modulations correspond directly to the modulation of a qubit. Thus, an eavesdropper has the additional and daunting task of determining which modulations correspond to actual qubit modulations before she can begin to extract any information from detected modulation states of the modulator.

WO 2006/047134 A3



— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

(88) Date of publication of the international search report:

12 July 2007

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US05/37352

A. CLASSIFICATION OF SUBJECT MATTER

IPC: **H04L 9/08**(2006.01)

USPC: 380/46,278

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. : 380/46,278²

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)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US PgPub 2004/0109564 A1 (Cerf et al.) 10 June 2004 (10.06.2004)	1-8

☐

Further documents are listed in the continuation of Box C.

☐

See patent family annex.

* Special categories of cited documents:		"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
"A"	document defining the general state of the art which is not considered to be of particular relevance	"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
"E"	earlier application or patent published on or after the international filing date	"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
"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)	"&"	document member of the same patent family
"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		

Date of the actual completion of the international search

02 April 2007 (02.04.2007)

Date of mailing of the international search report

08 MAY 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

Brandon S. Bludau

Telephone No. 571-272

