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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 July 2006 (13.07.2006)

PCT

(10) International Publication Number
WO 2006/074151 A3

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

(21) International Application Number:
PCT/US2006/000064

(22) International Filing Date: 3 January 2006 (03.01.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/030,241 6 January 2005 (06.01.2005) US

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **LAGASSE, Michael, J.** [US/US]; 6 Nautical Lane, Nahant, MA 01908 (US).

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

(88) Date of publication of the international search report:
28 May 2009

(54) Title: SECURE USE OF A SINGLE SINGLE-PHOTON DETECTOR IN A QKD SYSTEM

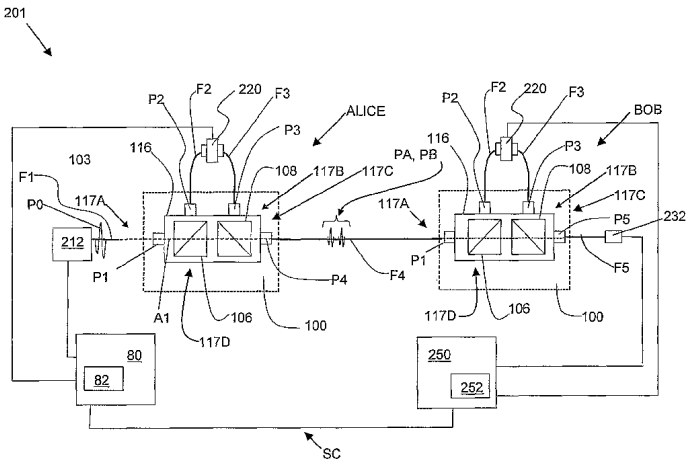

FIG. 4

(57) Abstract: A method of using a single single-photon detector (SPD) (232) in a quantum key distribution (QKD) system (101, 201) is described. The method includes modulating a phase of a quantum signal (PA, PB) a first time at a first QKD station (ALICE) by applying a first phase modulation randomly selected from a set of four possible phase modulations. The method also includes modulating the phase of the quantum signal a second time at a second QKD station (BOB). The second modulation involves applying a second phase modulation randomly selected from the same set of four possible phase modulations at the first QKD station. The method is a modification of the BB84 protocol and represents a higher level of quantum security than either the BB84 or B92 protocols when using a QKD system with a single SPD.

WO 2006/074151 A3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US06/00064

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

USPC: 380/256,259-260,263,277-278,283;398/40
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. : 380/256,259-260,263,277-278,283;398/40

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,307,410 (BENNETT) 26 April 1994 (26.04.1994), figures 2-3; column 5, lines 6-41; column 6, lines 30-63; column 10, lines 62-68; column 11, lines 1-7.	1, 3-4, 6-7 ---------- 2, 5
Y	US 6,529,601 B1 (TOWNSEND) 04 March 2003 (04.03.2003), column 10, lines 56-66.	2, 5
A	BENNETT et al., Generalized Privacy Amplification, IEEE Transactions on Information Theory, November 1995, Vol. 41, No. 6, pages 1915-1923.	1-7

☐ 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
05 June 2008 (05.06.2008)	15 JUL 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 MINH DINH Telephone No. 571-272-3000

Form PCT/ISA/210 (second sheet) (April 2007)

Continuation of B. FIELDS SEARCHED Item 3:
EAST (US-PGPUB, USPAT, EPO, JPO, DERWENT, IBM_TDB), INSPEC using following search terms: Quantum Key Distribution, phase modulation, beam splitter, error correction, private/privacy amplification.