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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 February 2008 (07.02.2008)

PCT

(10) International Publication Number
WO 2008/016201 A1

(51) International Patent Classification:
G02B 6/036 (2006.01)

(21) International Application Number:
PCT/KR2006/004087

(22) International Filing Date: 11 October 2006 (11.10.2006)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
10-2006-0072133 31 July 2006 (31.07.2006) KR

(71) Applicant *(for all designated States except US)*: **KOREA INSTITUTE OF SCIENCE AND TECHNOLOGY** [KR/KR]; 39-1 Hawolgok-2-dong, Sungbook-ku, Seoul 136-791 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOON, Sung-Wook** [KR/KR]; 404-1505 Booyoung Apt., Donong-dong, Namyangju, Kyungki-do 472-794 (KR). **PARK, Jun-Bum** [KR/KR]; #13, Jangmi, 242-128 Ungam-2-dong, Unpyung-ku, Seoul 122-915 (KR). **PARK, Chul-Woo** [KR/KR]; 401-17 Mangwoo-dong, Choonglang-ku, Seoul 131-230 (KR). **LEE, Kyung-Woon** [KR/KR]; 108-1107 Kuckdong Apt., Sadang-2-dong, Dongjak-ku, Seoul 156-772 (KR). **LEE, Seung-Hun** [KR/KR]; #201, 16-22 Yangjae-dong, Seocho-ku, Seoul 137-130 (KR). **SHIN, Hyun-Joon** [KR/KR]; 104-1709 Samsung Apt., Gongduck-2-dong, Mapo-ku, Seoul 121-762 (KR).

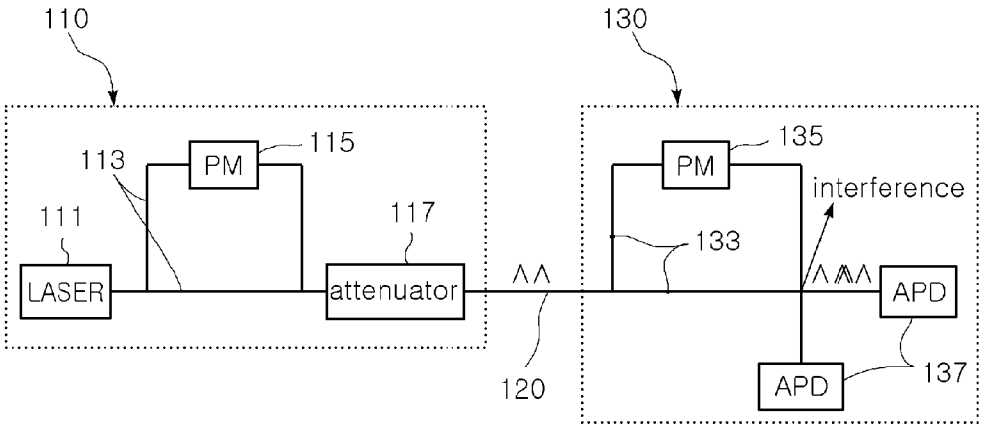
(74) Agent: **C & S LOGOS PATENT AND LAW OFFICE**; 13th Floor, Seocho-Pyunghwa Bldg., 1451-34 Seocho-dong, Seocho-gu, Seoul 137-070 (KR).

(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, KZ, LA, LC, LK, LR, LS, LT, LU, LV, 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),

[Continued on next page]

(54) Title: QUANTUM CRYPTOGRAPHY SYSTEM



(57) Abstract: Disclosed are a quantum cryptography system comprising a transmitting part and a receiving part. The transmitting part include a first optical fiber array of longer and shorter optical fibers for imparting a first path difference to an optical signal introduced from a light source, thereby dividing the optical signal into two signals having the first path difference, a first phase modulator for phase-modulating one of the signals propagating along the longer optical fiber and an attenuator for producing single photons respectively from the two signals, which are divided by the first path difference of the first optical fiber array. The receiving part includes a second optical fiber array of longer and shorter optical fibers for imparting a second path difference to the signals, which are received from the transmitting part through a quantum channel and have the first path difference, a second phase modulator for phase-modulating corresponding signal propagating along the longer optical fiber of the second optical fiber array and detector for detecting interferences between the signals outputted from the second optical fiber array. Each of the optical fibers of the transmitting part and the receiving part comprises a core containing B_2O_3 and the balance being SiO_2 and GeO_2, an inner cladding layer arranged around the core and composed of SiO_2 and at least one additive of F and P added to SiO_2 and an outer cladding layer arranged on the inner cladding layer and composed of SiO_2.

WO 2008/016201 A1

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*

Description

QUANTUM CRYPTOGRAPHY SYSTEM

Technical Field

[1] The present invention relates to a quantum cryptography system, more particularly, which employs a fiber optic material with very small thermal expansion in order to suppress phase shift according to temperature change and thus generate a correct quantum cryptography key.

[2]

Background Art

[3] The quantum cryptography system is a technology based on quantum mechanics, which modulates the phase of a single photon in order to share a secret key for encryption between transmitting and receiving parts. In such a quantum cryptography system, the secret key is determined by the interference of receipt signals of the receiving part, and thus it is important to maintain interference conditions of the receiving part stably.

[4]

[5] An example of the quantum cryptography system is illustrated in FIG. 1. As shown in FIG. 1, the conventional quantum cryptography system generally includes a transmitting part 10 and a receiving part 30, which are connected with each other through a quantum channel 20. The transmitting part 10 includes a light source 11, an optical fiber array 13 configured to impart a first path difference to an optical signal introduced from the light source 11, thereby dividing the optical signal into two signals having the first path difference, and a phase modulator 15 for modulating one of the optical signals propagating through a longer optical fiber of the optical fiber array 13. The receiving part 30 includes an optical fiber array 33 configured to impart a path difference to the optical signals received from the transmitting part 10 through the quantum channel 20, a phase modulator 35 for modulating corresponding optical signals propagating through a longer one of the optical fiber array 33 and a detector 37 for detecting an interference among the signals.

[6]

[7] Accordingly, the optical fiber array 13 divides a signal generated by the light source 11 of the transmitting part 10 into two signals. That is, one of the divided signals which is propagating along the longer optical fiber where the phase modulator 15 is located is modulated by the phase modulator 15. Then, owing to the resultant time delay corresponding to the length difference between longer and shorter optical fibers, the transmitting part 10 transfers two signals, the latter of which is modulated.

[8]

[9] When the two signals are transferred through the quantum channel 20, the first one of the two signals, which is not modulated, is divided again into two signals by the optical fiber array 33 of the receiving part 30. One of the divided signals which propagates along the longer optical fiber is modulated by the phase modulator 35. Then, the modulated signal interferes with the signal propagating along the shorter optical path owing to the phase difference, and the detector 37 detects an interference thereby generating a quantum cryptography key according to a preset protocol.

[10]

[11] However, in the conventional quantum cryptography system, any light dispersion under external physical force or phase shift according to temperature change may act as an obstacle against correct interference. This may act as a variable in the generation of quantum cryptography keys. For this purpose, the conventional quantum cryptography system is also provided with a heat insulator and a high precision temperature control system having 0.01℃ precision are added to the optical fiber portions of the transmitting and receiving parts. Even in this case, however, the degree of system stabilization is insignificant and thus there still exists an obstacle against the commercialization of such systems.

[12]

Disclosure of Invention

Technical Problem

[13] The present invention has been devised to solve the problem of phase shift according to temperature change in a conventional quantum cryptography system. Therefore an aspect of the invention to provide a quantum cryptography system which employs a phase stabilized fiber optic material for optical fibers in transmitting and receiving parts in order to solve the problem of phase shift according to temperature change.

[14]

[15] The present invention relates to a quantum cryptography system, more particularly, which utilizes a fiber optic material with very small thermal expansion in order to suppress phase shift according to temperature change and thus generate a correct quantum cryptography key.

[16]

Technical Solution

[17] According to an aspect of the invention, a quantum cryptography system includes a transmitting part including a first optical fiber array of longer and shorter optical fibers for imparting a first path difference to an optical signal introduced from a light source,

thereby dividing the optical signal into two signals having the first path difference, a first phase modulator for phase-modulating one of the signals propagating along the longer optical fiber and an attenuator for producing single photons respectively from the two signals, which are divided by the first path difference of the first optical fiber array; and a receiving part including a second optical fiber array of longer and shorter optical fibers for imparting a second path difference to the signals, which are received from the transmitting part through a quantum channel and have the first path difference, a second phase modulator for phase-modulating corresponding signal propagating along the longer optical fiber of the second optical fiber array and detector for detecting interferences between the signals outputted from the second optical fiber array.

[18]

[19] In this quantum cryptography system, each of the optical fibers of the transmitting part and the receiving part comprises a core containing B_2O_3 and the balance being SiO_2 and GeO_2, an inner cladding layer arranged around the core and composed of SiO_2 and at least one additive of F and P added to SiO_2 and an outer cladding layer arranged on the inner cladding layer and composed of SiO_2.

[20]

Brief Description of the Drawings

[21] FIG. 1 is a schematic diagram illustrating a conventional quantum cryptography system;

[22] FIG. 2 is a schematic diagram illustrating a quantum cryptography system according to an embodiment of the invention;

[23] FIG. 3 is a graph illustrating refractive index distribution of an optical fiber used in transmitting and receiving parts of the invention shown in FIG. 2; and

[24] FIG. 4 is a graph illustrating refractive index distribution of an exemplary fiber optic material of the invention having a F-rich inner cladding layer.

[25]

Best Mode for Carrying Out the Invention

[26] The present invention will now be described more fully hereinafter with reference to the accompanying drawings.

[27] FIG. 2 is a schematic diagram illustrating a quantum cryptography system according to an embodiment of the invention. Referring to FIG. 2, the quantum cryptography system of this embodiment includes a transmitting part 110 and a receiving part 130, which are connected with each other through a quantum channel 120.

[28]

[29] The transmitting part 110 includes a laser light source 111, a first optical fiber array 133 of longer and shorter optical fibers for imparting a first path difference to an optical signal introduced from the laser light source, thereby dividing the optical signal into two signals having the first path difference, a first phase modulator 115 for modulating the phase of one of the signals propagating along the longer optical fiber and an attenuator 117 for producing single photons respectively from the two signals, which are divided by the first path difference of the first optical fiber array 113.

[30]

[31] The receiving part 130 includes a second optical fiber array 133 of longer and shorter optical fibers for imparting a second path difference to the signals, which are received from the transmitting part 110 through the quantum channel 120 and have the first path difference, a second phase modulator 135 for modulating corresponding signals propagating along the longer optical fiber and detector 137 for detecting interferences between the signals outputted from the second optical fiber array 133.

[32]

[33] In the quantum cryptography system of this embodiment, the transmitting part 110 serves to impart a path difference to signals introduced from the laser light source 11 and provide such signals having the path difference to the receiving part 130 through the quantum channel 120. More particularly, a signal introduced from the laser light source 111 is divided into two signals through the first optical fiber array 113. That is, the signal is divided into one signal propagating along the longer optical fiber of the first optical fiber array 113 and the other signal propagating along the shorter optical fiber of the first optical fiber array 113, in which the signal propagating along the longer optical fiber is also modulated by the first phase modulator 115. Then, upon having exited the first optical fiber array 113, the two signals are converted respectively into single photons by the attenuator 117.

[34]

[35] Accordingly, those signals to be transferred from the transmitting part 110 include two signals having a time delay corresponding to the length difference between the longer and short optical fibers, the latter of which is modulated.

[36]

[37] The receiving part 130 allows the two signals received from the transmitting part 110 to propagate along the second optical fiber array 133 in order to impart a path difference to the signals. In the two signals transferred through the quantum channel 120, the first signal, which is not modulated is divided again into two signals by the second optical fiber array 133. One of the divided signals propagates along the longer optical fiber and then is modulated by the second phase modulator 135. The signal modulated by the second phase modulator 135 interferes with the signal propagating

along the shorter optical fiber of the second optical fiber array 133 owing to the phase difference between them. Then, the detector 137 detects the interference of the signals thereby generating a quantum cryptography key according to a preset protocol.

[38]

[39] In the quantum cryptography system of the above-described construction, the first optical fiber array 113 of the transmitting part 110 and the second optical fiber array 133 of the receiving part 130 are required to have the same magnitudes such as size and length so that the quantum cryptography key can be detected correctly.

[40]

[41] In addition, the optical fibers of the transmitting or receiving part can cause phase shift with its thermal expansion according to temperature change, thereby creating several problems to correct transmission of quantum cryptography keys. That is, a typical fiber optic material in use for optical communication includes a core of SiO_2 glass with a minor amount of GeO_2 doped thereto and a cladding layer of SiO_2 glass arranged around the core.

[42] Generally, the core has a higher refractive index than the cladding layer so that optical signals propagate along the core. However, the SiO_2 glass based fiber optic material thermally expands according to temperature, which may make it difficult to generate correct quantum cryptography keys when applied to the quantum cryptography system.

[43]

[44] Accordingly, a phase stabilized fiber optic material with its thermal expansion being substantially zero (0) is employed for the optical fibers of the transmitting and receiving parts 110 and 130 in order to prevent the phase shift according to temperature change.

[45]

[46] In detail, the fiber optic material of the invention contains a preset amount of B_2O_3 as a core component in addition to SiO_2 and GeO_2 so as to maintain the thermal expansion coefficient to be substantially 0. Preferably, B_2O_3 content is controlled at 2 to 10 Mol% with respect to SiO_2.

[47]

[48] In addition, the fiber optic material of the invention includes an outer cladding layer of SiO_2 arranged around the core, and further includes an inner cladding layer interposed between the core and the outer cladding layer. That is, unlike typical fiber optic materials, the fiber optic material of the invention has one more cladding layer arranged in the interior thereof in order to achieve single mode conditions. The inner cladding layer can act to control thermal expansion characteristics of the core while improving propagation characteristics of optical signals.

[49] In this invention, the inner cladding layer preferably contains at least one dopant of F and P added into SiO_2.

[50]

[51] More preferably, the dopant content is controlled to such a level that the refractive index of the inner cladding layer remains smaller than that of the outer cladding layer.

[52] FIG. 3 is a graph illustrating refractive index distribution of a fiber optic material used in an exemplary quantum cryptography system including a core, an inner cladding layer and an outer cladding layer. It can be appreciated that single mode conditions are satisfied in a wavelength range of 1200nm or more.

[53] FIG. 4 is a graph illustrating refractive index distribution of an exemplary fiber optic material of the invention having a F-rich inner cladding layer so that an inner cladding layer has a refractive index smaller than that of an outer cladding layer. The fiber optic material of this structure can control the thermal expansion characteristics of the core while promoting optical signal propagating performance.

[54]

Mode for the Invention

[55] The present invention will now be described with reference to the following Example.

[56]

[57] Example

[58] A quantum cryptography system as shown in FIG. 2 was prepared. In this system, a quantum channel length was 25Km, a signal transmission rate was 25.6kHz, and a detector having noise of 8×10^{-5} was used with an efficiency of 15%. In addition, the mean single photon of the detector was 0.2.

[59]

[60] For the optical fibers of the transmitting and receiving parts of the quantum cryptography system, a phase stabilized fiber optic material with substantially zero (0) thermal expansion according to temperature was used. In detail, the used fiber optic material included a core of SiO_2 doped with a specific amount of B_2O_3, and an inner cladding layer and an outer cladding layer of SiO_2 arranged sequentially on the core. The inner cladding layer contains a preset amount of F doped into SiO_2 so as to lower refractive index compared to that of the outer cladding layer.

[61]

[62] Detection was performed on the shift rate of cryptography keys for signaling generated by the detector in the quantum cryptography system of the above-described construction, and results are reported in Table 1 below in comparison with theoretical calculation results.

[63]

[64] Table 1

	Measured result	Theoretical calculation
R_{shift} (bit/s)	35+3	38.4
R_{error} (bit/s)	0.8±0.1	1.31
QBER(%)	2.3±0.3	3.3

[65]

[66] As reported in Table 1 above, it is appreciated that the shift rate R_{shift} of quantum cryptography keys generated by the detector according to a preset protocol is comparable with the theoretical calculation. It is also appreciated that the error rate R_{error} of the detector is within the theoretical calculation thereby generally satisfying the theoretical level.

[67]

[68] While the present invention has been described with reference to the particular illustrative embodiments and the accompanying drawings, it is not to be limited thereto but will be defined by the appended claims. It is to be appreciated that those skilled in the art can imitate or modify the embodiments into various forms without departing from the scope and spirit of the present invention.

[69]

Industrial Applicability

[70] As set forth above in this disclosure, the fiber optic material having substantially no thermal expansion can be used for the optical fibers of the transmitting and receiving parts in the quantum cryptography system. Due to this, the quantum cryptography system can be realized stably free from phase shift according to the temperature change in a temperature range from 0 to 30℃. Furthermore, this can improve the stability of an article as well as promote economic competitiveness thereof.

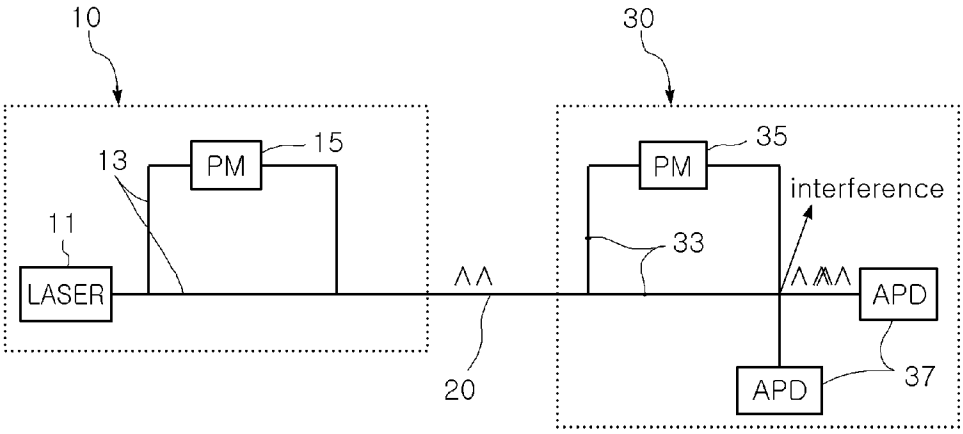
Claims

[1] A quantum cryptography system comprising:
a transmitting part including a first optical fiber array of longer and shorter optical fibers for imparting a first path difference to an optical signal introduced from a light source, thereby dividing the optical signal into two signals having the first path difference, a first phase modulator for phase-modulating one of the signals propagating along the longer optical fiber and an attenuator for producing single photons respectively from the two signals, which are divided by the first path difference of the first optical fiber array; and
a receiving part including a second optical fiber array of longer and shorter optical fibers for imparting a second path difference to the signals, which are received from the transmitting part through a quantum channel and have the first path difference, a second phase modulator for phase-modulating corresponding signal propagating along the longer optical fiber of the second optical fiber array and detector for detecting interferences between the signals outputted from the second optical fiber array,
wherein each of the optical fibers of the transmitting part and the receiving part comprises a core containing B_2O_3 and the balance being SiO_2 and GeO_2, an inner cladding layer arranged around the core and composed of SiO_2 and at least one additive of F and P added to SiO_2 and an outer cladding layer arranged on the inner cladding layer and composed of SiO_2.

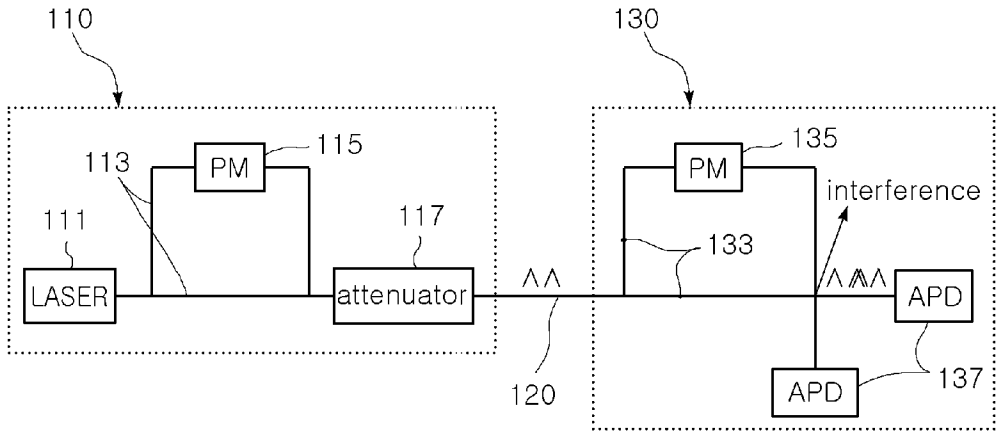
[2] The quantum cryptography system according to claim 1, wherein the core contains 2 to 10mol% of B_2O_3.

[3] The quantum cryptography system according to claim 1, wherein the inner cladding layer has a refractive index smaller than that of the outer cladding layer.

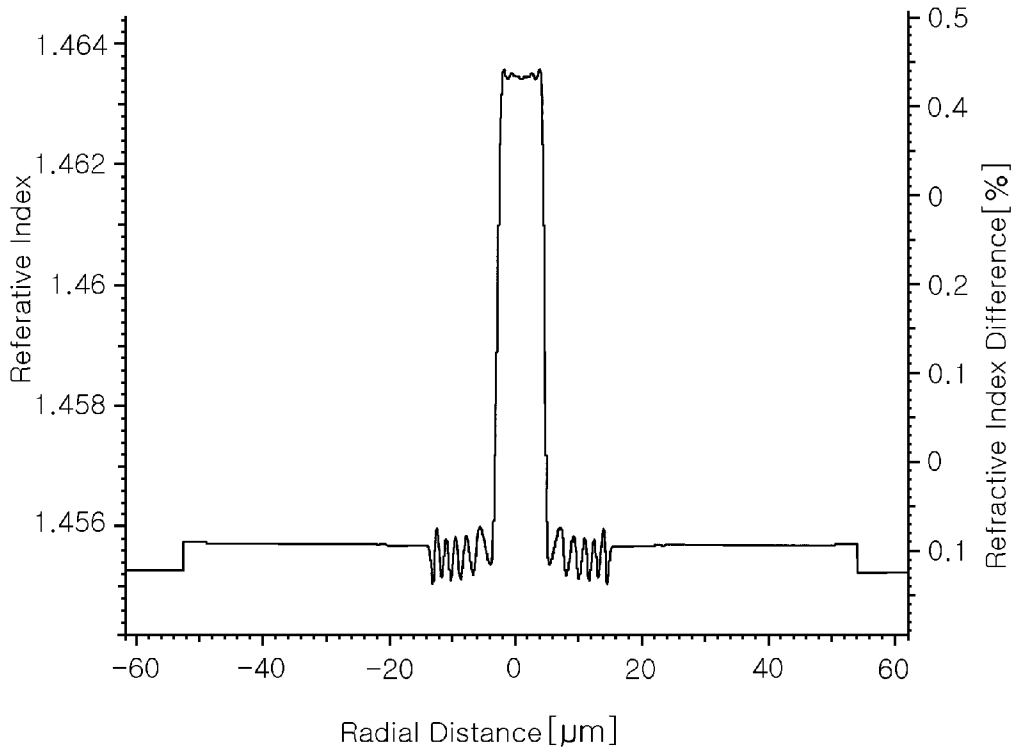
[Fig. 1]



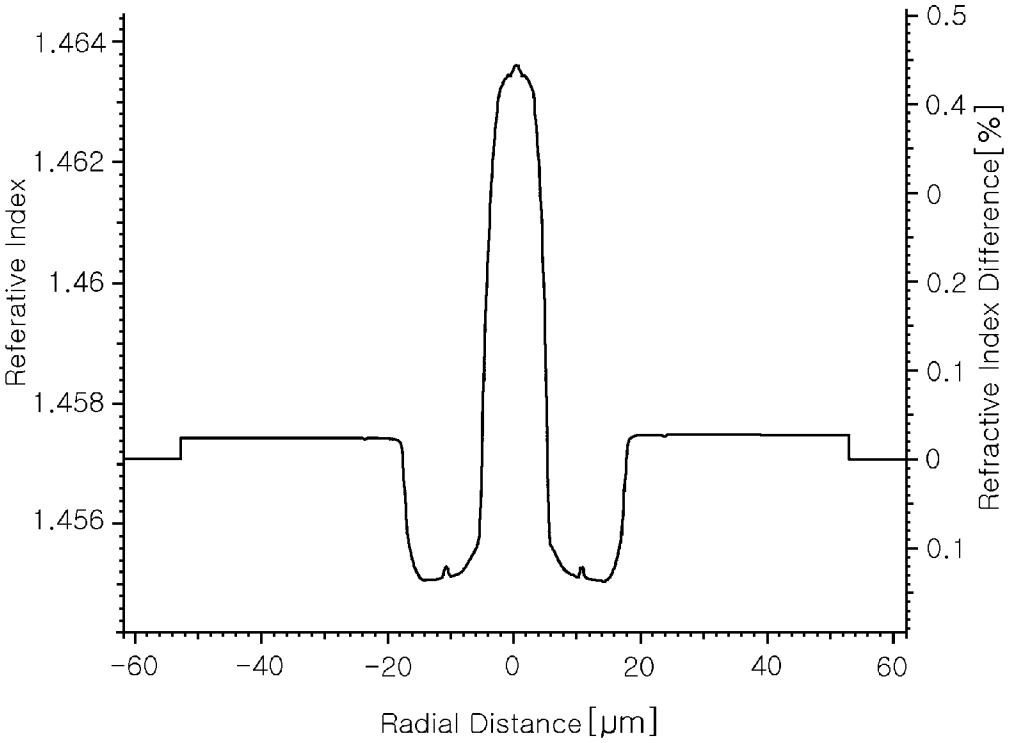
[Fig. 2]


110
130
PM
115
113
111
117
LASER
attenuator
120
PM
135
interference
133
APD
APD
137

[Fig. 3]


1.464
1.462
1.46
1.458
1.456
Referative Index
0.5
0.4
0
0.2
0.1
0
0.1
Refractive Index Difference[%]
−60
−40
−20
0
20
40
60
Radial Distance[μm]

[Fig. 4]


1.464
1.462
1.46
1.458
1.456
Referative Index
0.5
0.4
0
0.2
0.1
0
0.1
Refractive Index Difference[%]
-60
-40
-20
0
20
40
60
Radial Distance[μm]

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2006/004087

A. CLASSIFICATION OF SUBJECT MATTER

G02B 6/036(2006.01)i

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)
G02B 6/03

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Utility models and applications for Utility Models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKIPASS(KIPO internal)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,529,601B1 (PAUL D. TOWNSEND) 04 March 2003 See Fig.11 and claims.	1-3
A	US 6,678,431B2 (KI-HO HAN et al.) 13 January 2004 See Fig.10 and the abstract.	1-3
A	US 4,560,246B1 (DAVID COTTER) 24 December 1985 See Fig.1 and claims.	1-3
A	US 6,785,434 B2 (ANDREA CASTOLDI et al.) 31 August 2004 See Figs7,11 and the abstract	1-3

☐ 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 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 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
24 APRIL 2007 (24.04.2007)	**24 APRIL 2007 (24.04.2007)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	KOH, JAE HYUN Telephone No. 82-42-481-5687

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR2006/004087

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US06529601B1	04.03.2003	None	
US06678431B2	13.01.2004	KR1020030070225	29.08.2003
US4560246B1	09.06.1998	AT19449E	15.05.1986
		AU559570B2	12.03.1987
		BR8302963A	07.02.1984
		CA1216029A1	30.12.1986
		EP99632B1	23.04.1986
		FI74371C	11.01.1988
		HK50888A	15.07.1988
		IE54438B	11.10.1989
		IN158794A	24.01.1987
		JP2849700B2	20.01.1999
		KR9200163B1	09.01.1992
		NO167340C	23.10.1991
		PT76814B	27.02.1986
		ZA8303995A	29.02.1984
US6785434BB	31.08.2004	AU200131670A1	31.07.2001
		CA2397049AA	26.07.2001
		CN1395771A	05.02.2003
		EP1252729A1	30.10.2002
		JP15520987	08.07.2003
		KR1020020084092	04.11.2002
		WO200154318A1	26.07.2001