



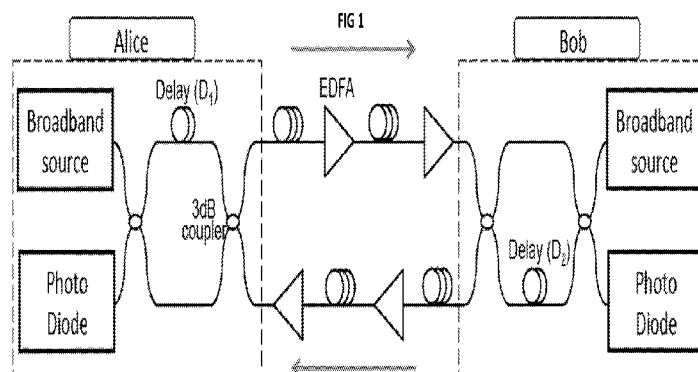
- (51) **International Patent Classification:**
H04B 10/2575 (2013.01) *H04B 10/25* (2013.01)
H04L 9/08 (2006.01)
- (21) **International Application Number:**
PCT/US2016/055282
- (22) **International Filing Date:**
4 October 2016 (04.10.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
62/240,030 12 October 2015 (12.10.2015) US
15/279,397 28 September 2016 (28.09.2016) US
- (71) **Applicant:** NEC LABORATORIES AMERICA, INC.
[US/US]; 4 Independence Way, Suite 200, Princeton, New
Jersey 08540 (US).
- (72) **Inventors:** WU, Ben; 1 Lawrence Drive, Princeton, New
Jersey 08540 (US). HUANG, Yue-Kai; 89 Hoover Avenue,
Princeton, New Jersey 08540 (US). YAMAN, Fatih;
1711 Northumberland Way, Monmouth Junction, New Jer-
sey 08852 (US).
- (74) **Agent:** KOLODKA, Joseph; NEC Laboratories America,
Inc., 4 Independence Way, Suite 200, Princeton, New Jer-
sey 08540 (US).

- (81) **Designated States** (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR,
KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ,
TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU,
TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,
DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU,
LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) **Title:** PHYSICAL LAYER KEY DISTRIBUTION FOR LONG DISTANCE REPEATED NETWORKS USING RANDOM ENVIRONMENTAL INSTABILITY



(57) **Abstract:** Aspects of the present disclosure describe methods and systems for improved secure key generation and distribution employing environmental instability induced signal phase fluctuations that are compatible with commercial wavelength division multiplexed (WDM) optical systems and associated optical amplifiers for long-haul transmission.

PHYSICAL LAYER KEY DISTRIBUTION FOR LONG DISTANCE REPEATED NETWORKS USING RANDOM ENVIRONMENTAL INSTABILITY

CROSS REFERENCE TO RELATED APPLCIATIONS

[0001] This application claims the benefit of United States Provisional Patent Application Serial No.62/240,030 filed 10/12/2015 the entire contents of which are incorporated by reference as if set forth at length herein.

TECHNICAL FIELD

[0002] This disclosure relates generally to systems and methods for secure encryption key generation and distribution and in particular to secure key distribution using environment instability induced signal phase fluctuations.

BACKGROUND

[0003] As is known, key distribution is an important consideration and characteristic required for network security.

[0004] Accordingly, given its importance to contemporary network security, methods, structures and apparatus that facilitate the secure distribution of such keys, would represent a welcome addition to the art.

SUMMARY

[0005] An advance in the art is made according to the present disclosure which describes methods and structures for improved secure key distribution. In sharp contrast to prior art methods, systems, and structures – and in particular software methods – methods, systems and structures according to the present disclosure is based on the instability of a fiber interferometer. According to an aspect of the present disclosure, keys are generated by an unstable effect which provides an asymmetric standing between communicating parties and eavesdropper. Communicating parties use the instability

directly for key generation and detection, while eavesdropper(s) introduce(s) extra instability such that the key(s) cannot be determined by the eavesdropper.

[0006] As compared with prior-art methods, systems and structures which have been incompatible with contemporary optical amplifiers and therefore cannot be transmitted over long distances, methods, systems and structures according to the present disclosure permit the generation and transmission of such keys over long distances.

[0007] Finally, and in further contrast to prior art methods, systems, and structures – which employed bidirectional transmission in a same fiber, methods, systems and structures according to the present disclosure employs a uni-directional transmission using two fibers, thus allowing methods, systems and structures according to the present disclosure compatible with uni-directional optical amplifiers that are used contemporaneously in long-haul terrestrial and submarine networks.

[0008] Advantageously, key distribution methods, systems and structures according to the present disclosure are compatible with both optical amplifiers for long-range transmission and can be implemented over existing fiber optic network with neighboring WDM channels. The key is generated from the fiber index fluctuation induced by the environmental instabilities - including temperature changes and mechanical vibrations.

[0009] Each communicating pair of fibers employ an interferometer to convert the combined environmental instabilities to phase signals. Broadband sources are used as a signal carrier to improve system security by minimizing signal coherence length.

Advantageously, security of the system relies on the fact that the light source has a short coherence length while a large optical delay difference is applied in the interferometers. Any eavesdropper would have to search for a large range optical delay in order to find a short coherence length. Moreover, even if an eavesdropper knows the optical delay, (s)he has to apply a same amount of delay to recover the phase information.

BRIEF DESCRIPTION OF THE DRAWING

[0010] A more complete understanding of the present disclosure may be realized by reference to the accompanying drawing in which:

[0011] **FIG 1** is a schematic block diagram illustrating an experimental setup according to an aspect of the present disclosure;

[0012] **FIGs 2(a)** and **2(b)** are a set of plots showing experimental measurement time domain signals received by **2(a)** Alice, and **2(b)** Bob for the experimental setup of **FIG 1** according to an aspect of the present disclosure;

[0013] **FIG 3** is a plot showing frequency domain signal received by Alice according to an aspect of the present disclosure.

[0014] The illustrative embodiments are described more fully by the Figures and detailed description. Inventions according to this disclosure may, however, be embodied in various forms and are not limited to specific or illustrative embodiments described in the Figures and detailed description

DESCRIPTION

[0015] The following merely illustrates the principles of the disclosure. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the disclosure and are included within its spirit and scope.

[0016] Furthermore, all examples and conditional language recited herein are principally intended expressly to be only for pedagogical purposes to aid the reader in understanding the principles of the disclosure and the concepts contributed by the inventor(s) to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions.

[0017] Moreover, all statements herein reciting principles, aspects, and embodiments of the disclosure, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

[0018] Thus, for example, it will be appreciated by those skilled in the art that any block diagrams herein represent conceptual views of illustrative circuitry embodying the principles of the disclosure. Similarly, it will be appreciated that any flow charts, flow diagrams, state transition diagrams, pseudo code, and the like represent various processes which may be substantially represented in computer readable medium and so executed by a computer or processor, whether or not such computer or processor is explicitly shown.

[0019] The functions of the various elements shown in the Figures, including any functional blocks labeled as "processors", may be provided through the use of dedicated hardware as well as hardware capable of executing software in association with appropriate software. When provided by a processor, the functions may be provided by a single dedicated processor, by a single shared processor, or by a plurality of individual processors, some of which may be shared. Moreover, explicit use of the term "processor" or "controller" should not be construed to refer exclusively to hardware capable of executing software, and may implicitly include, without limitation, digital signal processor (DSP) hardware, network processor, application specific integrated circuit (ASIC), field programmable gate array (FPGA), read-only memory (ROM) for storing software, random access memory (RAM), and non-volatile storage. Other hardware, conventional and/or custom, may also be included.

[0020] Software modules, or simply modules which are implied to be software, may be represented herein as any combination of flowchart elements or other elements indicating performance of process steps and/or textual description. Such modules may be executed by hardware that is expressly or implicitly shown.

[0021] Unless otherwise explicitly specified herein, the FIGs comprising the drawing are not drawn to scale.

[0022] By way of some additional background, we again note that oftentimes Network security relies on data encryption occurring between signal transmitters and receivers. One fundamental enabler of such data encryption is the secure generation and distribution of an encryption key. If the encryption key is attacked and exposed to an eavesdropper, an encrypted signal may be easily decrypted.

[0023] Traditional key generation schemes and systems constructed therefrom are oftentimes based on software algorithms. For example, the Rivest-Shamir-Adleman (RSA) cryptosystem, is based on the fact that it is difficult to factor the product of two large prime numbers [See, e.g., R. L. Rivest, et al, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM 21, 120-126 (1978)]. The security of the system relies on computation resources available for the eavesdropper, while the increasing power of quantum computing raises a potential challenge to the software-based key generation schemes (See, e.g., P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," SIAM J. COMPT. 26,1484-1509 (1997)).

[0024] In contrast to such software systems, physical layer key generation schemes are known as alternative approaches for encryption systems. One such scheme - quantum key distribution (QKD) - has been widely studied as a secure key distribution system [See, e.g., H. K. Lo, et al, "Secure quantum key distribution," Nature Photonics 8, 596-604 (2014)].

[0025] The overall security of a QKD system relies – in part - on the fact that an eavesdropper cannot measure the signal, which is a quantum state of a single photon without knowing the eigenvalues of the quantum states. Compared with software based key distribution, QKD has the advantages that if an eavesdropper records the wrong

quantum state, the original signal is lost and changed, and the eavesdropper cannot use post-processing techniques to recover the signal.

[0026] Although QKD has been demonstrated to be secure, the deployment of a QKD system has practical issues. First, the QKD system requires single photon transmission, which means the signal cannot be amplified by standard optical amplifiers. As will be readily understood by those skilled in the art, such a restriction limits the transmission distance within 100-200km without regeneration. Second, due to the extreme sensitive nature of the single photon detection, a QKD scheme is not compatible with standard commercial wavelength division multiplexing (WDM) systems.

[0027] With this further background in place, we note that according to the present disclosure – we demonstrate a key distribution method and structure(s) that is compatible with optical amplifiers for long- range transmission. Of particular advantage, such a key distribution scheme according to the present disclosure may be implemented using existing fiber optic network(s) having neighboring WDM channels.

[0028] The key is generated from the fiber index fluctuation induced by the environmental instabilities including temperature changes and mechanical vibrations (See, e.g., K. Kravtsov, et al, "Physical layer secret key generation for fiber-optical networks," Opt. Express 21, 23756-23771 (2013)). Each of the communicating pair employs an interferometer to convert the combined environmental instabilities to phase signals.

[0029] Broadband sources are used as the signal carrier to improve system security by minimizing signal coherence length. The security of the system relies on the fact that the light source has short coherence length while large optical delay difference is applied in the interferometers. Accordingly, an eavesdropper would have to search over a large range optical delay in order to find a short coherence length. Moreover, even if the eavesdropper knows the optical delay, (s)he has to apply same amount of delay to recover phase information. Furthermore, any extra delay that the eavesdropper uses also

generates phase changes from environmental instabilities and adds phase randomness to the measured key signal.

[0030] **FIG. 1** is a schematic diagram illustrating a structure for a key distribution scheme according to an aspect of the present disclosure. As may be observed, the illustrative structure includes two Mach-Zehnder (MZ) delayed interferometer(s). The two MZ interferometers each include a delay loop (D1 and D2) that provides a delay to a respective MZ interferometer. The two MZ interferometers are optically connected to one another (output of one to input of the other and vice versa) via a “transmission span” including one or more length(s) of optical fiber and one or more optical amplifiers, i.e., erbium-doped fiber amplifier(s) (EDFA). A key signal is derived from phase fluctuation in the fiber interferometer.

[0031] As depicted in that illustration shown schematically in **FIG. 1**, there are shown the two MZ interferometers – used illustratively by Alice and Bob. As will be readily appreciated with respect to this illustration, both Alice and Bob send and receive signals exhibiting phase(s) affected by local temperature changes and mechanical vibrations. Since signals in both directions traverse the same physical paths, the interference results at the MZ Interferometer outputs will be the same at both ends, thus enabling key sharing.

[0032] Shown further in that figure, broadband sources are used as signal carriers to prevent eavesdropper(s) from measuring the phase directly with – for example - coherent detection mechanisms. In the illustrative scenario depicted in the figure, both Alice and Bob use a filtered amplifier spontaneous emission (ASE) from erbium doped fiber amplifier (EDFA) with bandwidth of substantially 1500Hz and a center wavelength at 1547.6nm as the light source. Since the broadband source has a short coherence length, the optical delay from Alice (L1) and Bob (L2) is matched to within a few millimeters to recover the phase information.

[0033] In the illustrative configuration shown in **FIG. 1**, the optical delay we used ranges from 20m to 26km, which means without information about the optical delay

used, the eavesdropper has to scan the optical delay and search for a few millimeter ranges in the range of 26km to find the coherence length. Even if an eavesdropper is able to somehow find the right optical delay, (s)he still needs an interferometer that matches the delay and generates new phase randomness in addition to the phase information (s)he wants to measure. In a case such as the one described, an eavesdropper can never precisely measure the phase information.

[0034] With further reference to **FIG. 1**, we note that the basic structure – the two MZ interferometers of Alice and Bob, are employed to generate a key signal due to the instability of the two optical delays (D1 and D2) positioned in the interferometer(s), respectively. Since the phases of the signals traversing the optical fibers are very sensitive to many environmental parameters including temperature, mechanical vibrations, and acoustic waves, the accumulated phase differences in the optical delays are random and difficult to predict by measuring the environmental parameters. The phase differences generated by the optical delay pairs (D1 and D2) create different states of interferences (between constructive and destructive) between the signals with identical path length. Since the optical signal generated from Alice and Bob pass through the same optical delay pairs, Alice and Bob receive the same interference result. Advantageously, and as can surely be appreciated by those skilled in the art, the interference result can then be used as a key distributed secretly between Alice and Bob.

[0035] Advantageously, optical broadband sources are used in key distribution scheme(s) – according to the present disclosure, so an eavesdropper cannot measure the phase directly. The bandwidth(s) of optical sources may be orders of magnitude larger than the bandwidth of any commercially available coherent receivers so it will be largely impossible to store all of the optical signal information digitally for additional signal processing. Since the broadband sources exhibit short coherence length(s), in order for an eavesdropper to observe the effect of the phase change (s)he will need to match the optical delay within the coherence length of the broadband sources. However, the coherence length of the broadband source(s) range from sub-millimeter to centimeters – depending on the spectral width – while several tens of kilometers of optical delays can be easily applied by Alice and Bob. Accordingly, without information about the optical

delay, the eavesdropper has to match the length down to several millimeters in resolution over a range of tens of kilometers. Even if an eavesdropper can match the length of the optical delay, the MZI (s)he uses will also generate phase instability at the same order of magnitude as the phase difference that (she) needs to measure. The uncertainty of this measurement is as large as the signal to be measured, thus rendering the attack ineffective.

[0036] Notably, we have demonstrated the transmission of a key distribution channel – according to the present disclosure - using a standard C-band transmission window. The 240-km bi-directional fiber-pair link includes three 80-km single mode fiber (SMF) spans, with erbium-doped fiber amplifier (EDFA) to compensate the average fiber loss of 17.5 dB. Thirty-eight (38) dummy WDM channels were emulated by carving a broadband source using a flexible-band wavelength selective switch (WSS) at 100-GHz spacing. Advantageously, our key distribution scheme was verified in this 240-km long WDM link, achieving a key-rate of 100bps and pre-coded key error rate of only 0.5%.

[0037] **FIG. 2(a)** and **FIG. 2(b)** are plots illustrating time domain signal(s) received by Alice and Bob, respectively. The signals shown have their intensities normalized and the comparison of the signal received by Alice and Bob shows that they have indeed received the same waveform due to the joint measurement of phase instability due to MZI. These analog signals can be further digitized to generate key shared by Alice and Bob. The length of the key sequence depends on number of levels in each time sample.

[0038] As will be appreciated, **FIG. 2(a)** and (b) demonstrates a system according to the present disclosure having back-to-back transmission and an optical delay of 20m. The Fourier transform of the signal received by Alice shows that the changing speed is several hertz (See, e.g., **FIG. 3**). To increase the key generation speed, longer optical delay (up to tens of km) may be used to increase the speed of phase fluctuation in MZI, wherein the key generation speed is proportional to the length of the optical delay.

[0039] As will be appreciated by those skilled in the art with respect to the illustrative configuration and results shown - when 26km optical delay is applied by Alice and Bob, the direct detection of the interference results matches in the situation where back-to-back transmission is employed, and when the signal is transmitted over 240km, the signals do not match. This is because the key distribution between Alice and Bob is based on the assumption that when the signal is transmitted from Alice to Bob, the environmental condition has to remain the same, so the signal transmitted from Bob to Alice has the same phase change. In the case of 240km transmission, phase change occurs in less than 1ms, while it takes the light signal 1.2ms to traverse 240km in the fiber. The signals in the dual directions experience different phase changes.

[0040] Note that although using a shorter optical delay can match the signal between Alice and Bob, it will make it easier for the eavesdropper to find the optical delay. Since the speed at which the changing of the phase is proportional to the optical delay length in the interferometer, a slower changing phase give the dual direction signal enough time to transmit between Alice to Bob and therefore undergo the same amount of phase change. However, the eavesdropper can use coherence detection to measure part of the signal spectrum and the fringes in the spectrum indicate the optical delay difference (see, e.g., **FIG. 3**). To find the fringes, the temporal data collected by the eavesdropper needs to be long enough so the Fourier transform of the temporal data, which is a spectrum, has the resolution to observe the fringes. While on the other side, if the eavesdropper collects data so long that the phase has changed, the fringes will shift and average to a constant.

[0041] Accordingly, to prevent the eavesdropper's attack, the optical delay difference has to be long enough to enable the phase change before the eavesdropper collects the temporal data. Moreover, a longer optical delay difference corresponds to a narrower fringe, which means the eavesdropper needs a higher spectrum resolution and longer temporal data. In our experimental configuration, we perform the coherence detection as an eavesdropper to attack the system. We found that the optical delay has to be in the order of 26km for the fringes to disappear (**FIG. 3**).

[0042] Notably, the fast changing phase from the long optical delay protects the system from attack, while it also leads to signal mismatch between Alice and Bob. To match the signal, the fast changing component of the phase has to be removed and the slow changing component of the phase can be used as key distribution. Since the direct detection of the interference signal is the cosine of the phase, and cosine is not a monotonic function, the sine of the phase is needed to recover the phase. We used a phase modulator that switches between 90° and 0° at a rate of 100kHz - which is more than 10 times faster than the phase changing rate. In this case, both sine and cosine of the phase can be measured, so the original phase can be recovered. A low pass filter with 3dB cutoff frequency 125Hz is applied to the phase signal and Figs. 4 (c) and (d) shows that the cosine of the filtered phase signal matches. The cross correlation of Alice's and Bob's signal reached to 0.8 at 0 delay and drop to 0 when the delay is not matched, which means the signal is truly random.

[0043] To extract the key from the analog signal, we set a buffer region in the middle and the sampled point is dropped if it falls in the buffer region. Two level digitization is applied and both sine and cosine of the phase can be used to generate keys. The key generation rate is 100bps with error rate of only 0.5%. To increase the key rate, the shape of the waveform can be considered for multi-level digitization.

[0044] As is now apparent to those skilled in the art, we have described and experimentally evaluated a key distribution system based on environmental instabilities. Advantageously, the key signal can be amplified by EDFAs and 240km bi-directionally transmission has been demonstrated. The key distribution channel shares the C-band transmission spectrum with 38 neighboring WDM channels. The system generates key at the rate of 100bps with error rate of 0.5%. To attack the system, an eavesdropper has to search for the coherence length of a few millimeters in the range of 26km. The fast changing phase from the long optical delay prevent the eavesdropper from measuring optical delay by the fringes of the spectrum.

[0045] At this point, while we have presented this disclosure using some specific examples, those skilled in the art will recognize that our teachings are not so limited.

Accordingly, this disclosure should be only limited by the scope of the claims attached hereto.

Claims:

1. A method of secure key generation in an optical communications system comprising a communicating pair of nodes, each node including a Mach-Zehnder Interferometer (MZI), each MZI including an optical delay loop in one of its arms, wherein the communicating pair of nodes are optically interconnected by a bidirectional fiber-pair link, said method of secure key generation comprising:
 - generating the secure key from only physical layer characteristics of the communications system; and
 - conveying that generated key from one of the nodes to the other.
2. The method of claim 1 wherein the key is generated from fiber index fluctuation induced by environmental instabilities.
3. The method of claim 2 wherein the environmental instabilities include temperature changes and mechanical vibrations.
4. The method of claim 3 wherein the environmental instabilities are converted to phase signals through the effect of the MZI in a particular node.
5. The method of claim 4 wherein the optical delay is $\geq 20\text{m}$ and $\leq 26\text{km}$.
6. The method of claim 5 wherein the bidirectional fiber-pair link optically connecting the nodes is $> 200\text{Km}$ in length.
7. The method of claim 6 wherein the optical communications system employs wavelength division multiplexing (WDM).
8. The method of claim 7 wherein the bidirectional fiber-pair link optically connecting the nodes includes one or more erbium-doped fiber amplifiers.

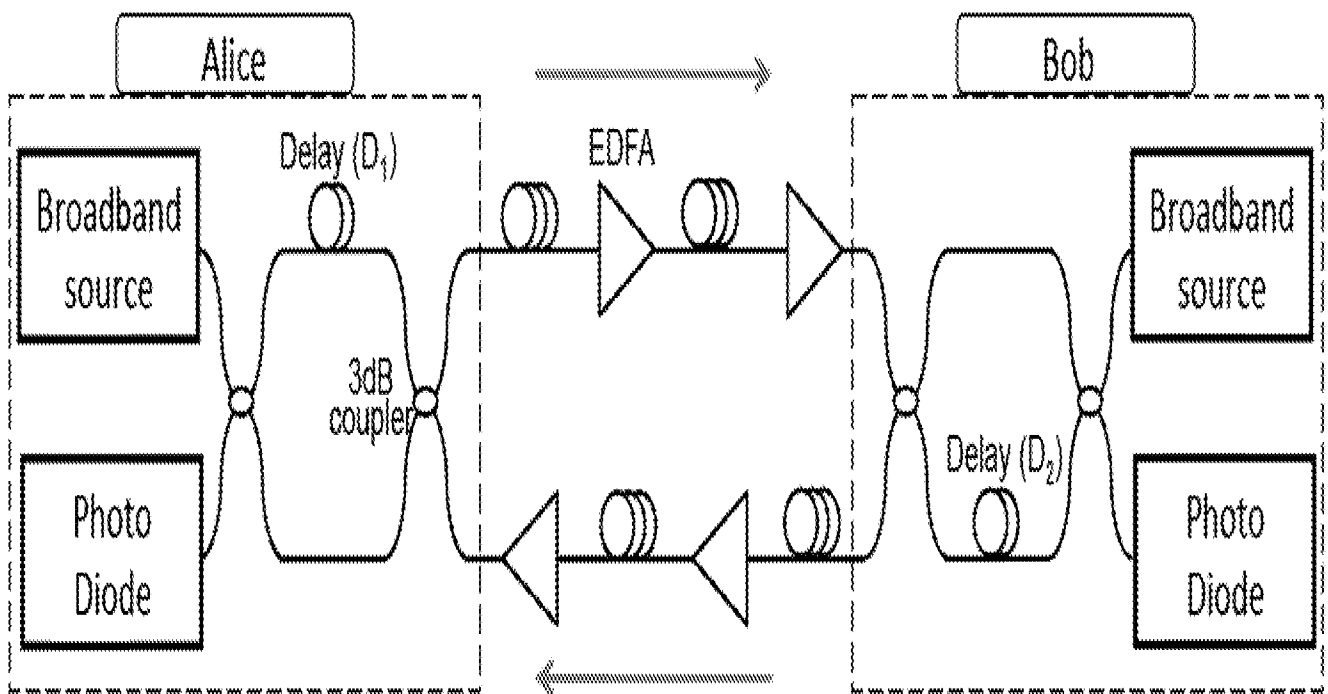


FIG 1

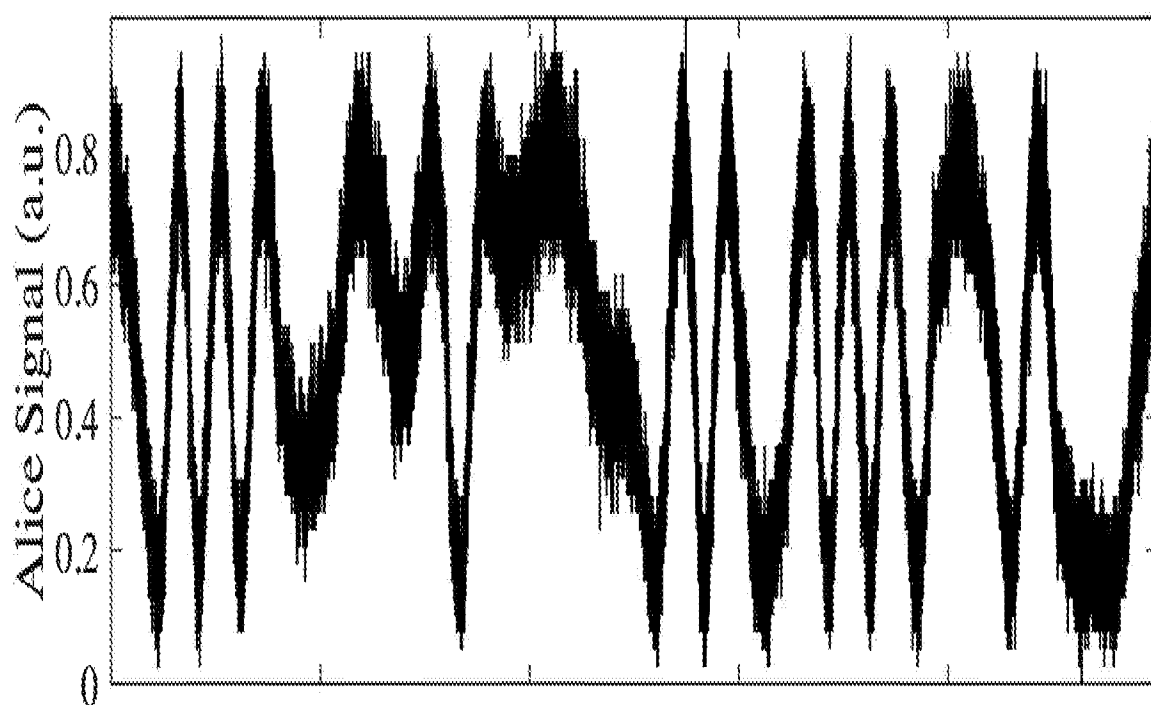


FIG 2(A)

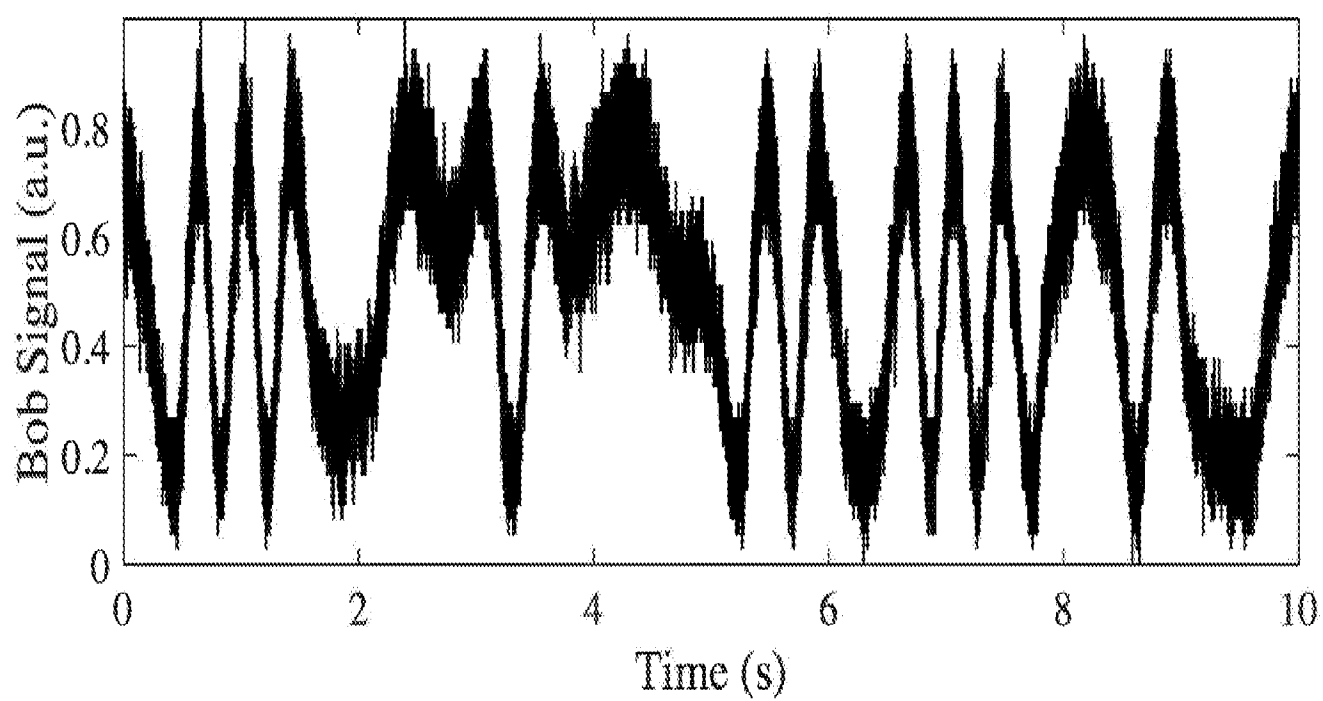


FIG 2(B)

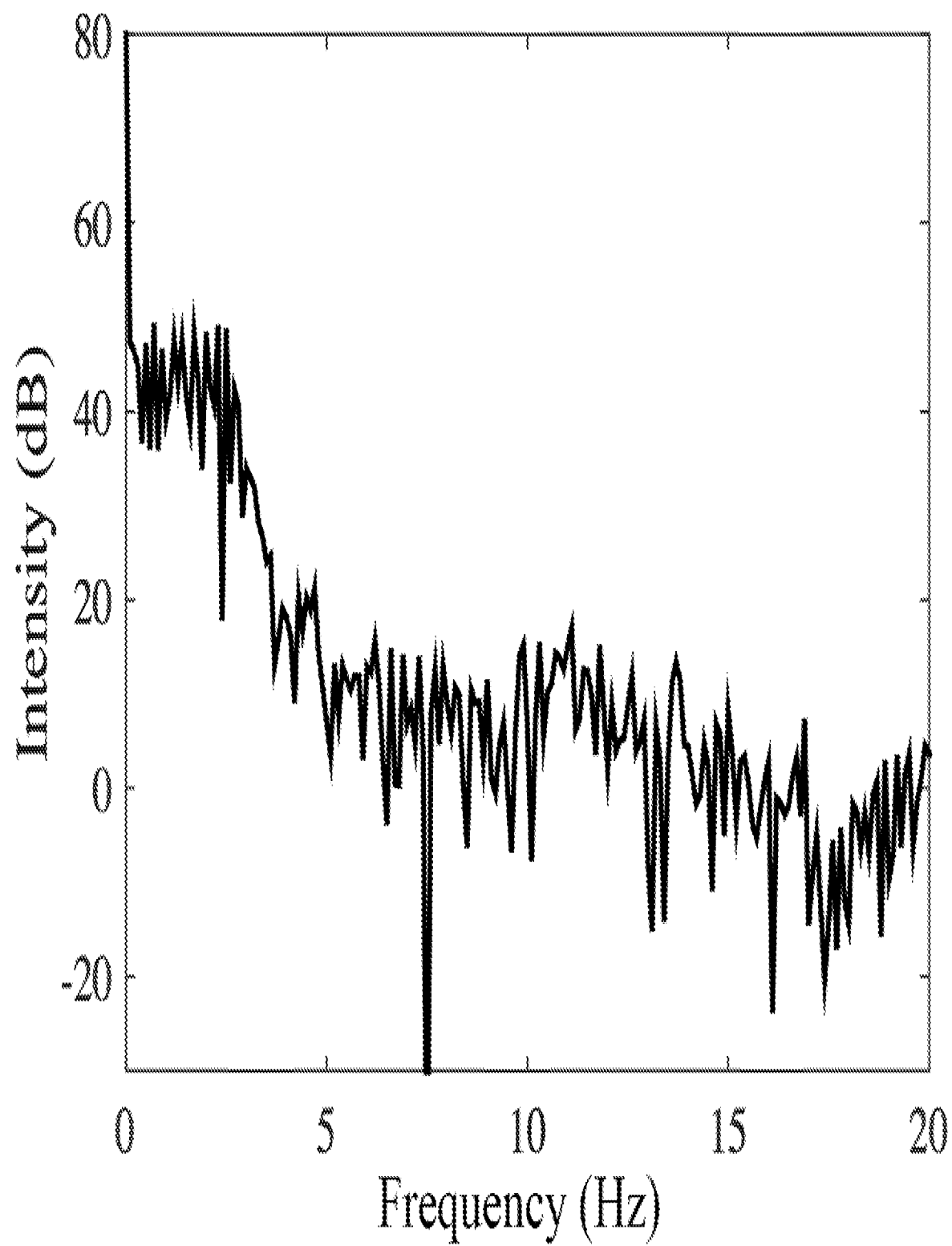


FIG 3

A. CLASSIFICATION OF SUBJECT MATTER**H04B 10/2575(2013.01)i, H04L 9/08(2006.01)i, H04B 10/25(2013.01)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)

H04B 10/2575; H04L 9/08; H04K 1/00; H04L 9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & keywords: secure key generation, Mach-Zehnder Interferometer (MZI), optical delay loop, arm, bidirectional fiber-pair link, physical layer characteristics, environmental instabilities, temperature changes, mechanical vibrations, WDM, erbium-doped fiber amplifiers

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KONSTANTIN KRAVTSOV et al., 'Physical layer secret key generation for fiber-optical networks', In: OPTICS EXPRESS, vol.21, No. 20, 30 September 2013 (https://www.osapublishing.org/oe/fulltext.cfm?uri=oe-21-20-23756&id=268539) See abstract; sections 1.1-3.3; and figure 5.	1-6
Y		7,8
Y	US 2011-0280405 A1 (JONATHAN LENAHAH HABIF) 17 November 2011 See paragraphs [0044]-[0047]; and figure 7.	7,8
A	US 2011-0150226 A1 (JEONG-SIK CHO) 23 June 2011 See paragraphs [0046]-[0048]; and figure 4.	1-8
A	US 2006-0239463 A1 (JONATHAN YOUNG) 26 October 2006 See paragraphs [0022]-[0034]; and figure 1.	1-8
A	US 6438234 B1 (NICOLAS GISIN et al.) 20 August 2002 See column 2, lines 33-62; and figure 1.	1-8



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 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

05 January 2017 (05.01.2017)

Date of mailing of the international search report

13 January 2017 (13.01.2017)

Name and mailing address of the ISA/KR

International Application Division

Korean Intellectual Property Office

189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

KANG, Hee Gok

Telephone No. +82-42-481-8264



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2016/055282

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0280405 A1	17/11/2011	US 8433070 B2	30/04/2013
US 2011-0150226 A1	23/06/2011	KR 10-1327661 B1	14/11/2013
		KR 10-2011-0071803 A	29/06/2011
		US 8477947 B2	02/07/2013
US 2006-0239463 A1	26/10/2006	CN 101502037 A	05/08/2009
		EP 1872509 A2	02/01/2008
		EP 1872509 A4	07/12/2011
		EP 1872509 B1	11/07/2012
		JP 2008-538680 A	30/10/2008
		US 8098826 B2	17/01/2012
		WO 2006-115846 A2	02/11/2006
		WO 2006-115846 A3	16/04/2009
US 6438234 B1	20/08/2002	AT 258733 T	15/02/2004
		AU 4206897 A	26/03/1998
		CA 2265553 A1	12/03/1998
		CA 2265553 C	13/03/2007
		CZ 295335 B6	13/07/2005
		CZ 9900477 A3	11/08/1999
		DE 69727388 T2	25/11/2004
		DK 0923828 T3	24/05/2004
		EP 0923828 A1	23/06/1999
		EP 0923828 B1	28/01/2004
		ES 2215238 T3	01/10/2004
		JP 04095672 B2	04/06/2008
		JP 2000-517499 A	26/12/2000
		WO 98-10560 A1	12/03/1998