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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 August 2016 (04.08.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/119867 A1

(51) International Patent Classification:
*H04L 9/08* (2006.01) *H04L 9/12* (2006.01)

(21) International Application Number:
PCT/EP2015/051855

(22) International Filing Date:
29 January 2015 (29.01.2015)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **FRAUNHOFER-GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V.** [DE/DE]; Hansastraße 27c, 80686 München (DE).

(72) Inventors: **PERLOT, Nicolas**; Cunostr. 54A, 14193 Berlin (DE). **RÖDIGER, Jasper**; Behmstr. 46, 13357 Berlin (DE).

(74) Agents: **SCHENK, Markus** et al.; Schoppe, Zimmermann, Stöckeler, Zinkler, Schenk & Partner mbB, Radlkoferstrasse 2, 81373 München (DE).

(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, 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, 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: CRYPTOGRAPHIC KEY DISTRIBUTION BASED ON TURBULENCE-INDUCED BEAM FLUCTUATIONS

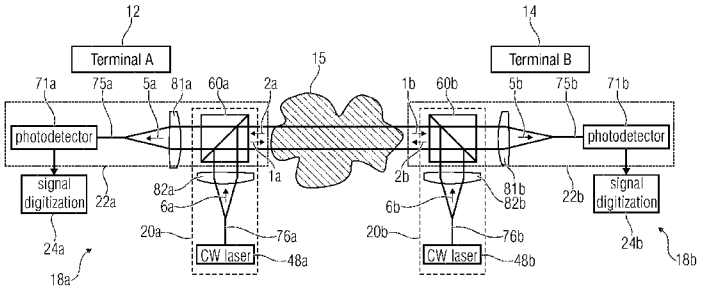


FIG 9

(57) Abstract: The distribution of a cryptographic key exploiting the randomness and reciprocity offered by turbulence is secure on the one hand and, on the other hand, is implemented more easily by way of the following measure: optical beams are mutually sent to one another through turbulence with exploiting the reciprocity of the deformed transverse optical fields of the mutually sent probe beams, the deformation being random and subject to reciprocity. A one-time travel of the optical beams is sufficient thereby alleviating adjustment precision requirements and saving a mirror for a back travel of the beams, respectively.

WO 2016/119867 A1

# Cryptographic Key Distribution based on Turbulence-induced Beam Fluctuations

## Description

The present application is concerned with cryptographic key distribution based on turbulences.

Encryption is an important topic in modern communication. The widest used method uses complex encryption algorithms with the disadvantage that, with fast enough classical computers or not yet usable quantum computers, decryption is possible in a reasonable time period.

A more secure method uses a one-time pad (OTP), a key, only known to the sender and receiver of a secret message. This key is at least as long as the message and is only used once to prevent an eavesdropper from getting information about it. The encrypted message itself can then be sent over a public channel. Therefore, a secure method of sharing a new secret key every time one wants to send a secret message is needed. One solution is to use quantum key distribution (QKD) [1], where the security of the code is ensured by the no-cloning theorem of quantum physics. But QKD systems are complex to implement. In particular, QKD requires special components, such as single-photon sources and/or detectors that are expensive and delicate to handle.

In recent years methods to distribute a secret key without using quantum effects have been proposed. In the present invention, security comes firstly from the unpredictable changes of the channel that randomly modulates the emitted wave, and secondly, from the practical impossibility for an eavesdropper to measure these unpredictable changes.

Conventionally, random-channel key distributions use the fluctuations of longitudinal phase (i.e. phase in the direction of propagation) to generate the key signals. Several physical channels can be used: radio, fiber optics, free-space optics.

In radio communication, using the wireless channel as a random source for key distribution is well-known [5]-[7]. However, because of the longer wavelength used in radio frequency, only large spatial variations, compared to the centimeter scale of optical

turbulence, affect the signal. The randomness of the radio channel involves e.g. the position of reflectors (such as vehicles).

A phase-changing character of optical fibers is used in [2]. Two optical fibers connect the two parties and form the two arms of a large-scale Mach-Zehnder-Interferometer that allows the measurement of the phase difference induced in these two arms. The method relies on the channel reciprocity where both parties measure the same phase difference which constitutes the secret key as phase measurement.

Fiber connection is, however, cumbersome. Using FSO, we measure the variations of the wavefront rather than the longitudinal phase. This greatly simplifies the measurement apparatus as there is no need to make two optical signals interfere. The FSO version requires only two coupling telescopes, one at each end.

Atmospheric turbulence can randomly modulate the phase [3][4] of a free-space optical (FSO) laser beam. The use of turbulence over an FSO link to generate a random key is proposed in Refs [3][4]. They describe a method where each of the two parties has a terminal that sends a laser beam to the other. Each beam is reflected back to the respective sender and the longitudinal phase difference between the transmitted and received beams is measured to create the key. The method based on longitudinal-phase measurements has several disadvantages. It is complex because each terminal must receive and reflect a beam. There has to be a mirror at both terminals. A coherent detection and expensive optical components are necessary. Furthermore, the laser travels two times the link distance, which leads to much higher propagation losses and therefore reduces the maximum link distance.

It is the object of the present invention to provide a secure and easier-to-implement concept for cryptographic key distribution using random wavefront-distorting medium.

This object is achieved by the subject matter of the enclosed independent claims.

It is a basic finding of the present invention that the distribution of a cryptographic key exploiting the randomness and reciprocity offered by a random wavefront-distorting medium is secure on the one hand and, on the other hand, may be implemented more easily if optical beams are mutually sent to one another through the random wavefront-distorting medium with exploiting the reciprocity of transverse optical fields of the

deformed wavefront of mutually sent probe beams, the deformation being random and subject to reciprocity. A one-time travel of the optical beams is sufficient as the received transverse optical field is inspected. Thereby, adjustment precision requirements are alleviated and a mirror for a back travel of the beams is saved.

In other words, embodiments of the present invention exploit that it is feasible to use a turbulent channel in a simple and cheap manner to create and distribute a secret cryptographic key. The key distribution is sufficiently installed if two terminals or two parties mutually send to/from each other a probe signal such as a laser beam while the cryptographic key is contained in, and accordingly derived from, the fluctuations of the received amplitude and phase front of the received optical field at each terminal. Both parties use the same spatial channel for reception and transmission so as to form a pair of reciprocal channels between both parties, respectively, and because of the channel reciprocity in both directions, they measure the same fluctuations which are characteristic of this particular channel and, therefore, can be used to create a secure cryptographic key. An eavesdropper, called Eve, hardly gets access to the cryptographic key at least because of the following combined technical difficulties. For example,

1) Eve would try to capture the two transverse fields over the area where the spatial correlation (or a function thereof) can be calculated. This area is the largest in the middle of a symmetrical link.
2) Eve should try to capture each of the two transmitted fields in the same, or almost the same, transverse plane.
3) Eve would hardly success in precisely superposing and coherently detecting the two captured fields.

Changes in turbulent channels induce fluctuations in the received optical field on a millisecond scale. Accordingly, embodiments of the present application allow for generating the cryptographic key at a symbol rate in the kHz scale. The requirements imposed onto the receivers are low. No fast (therefore expensive) receivers/detectors are needed. The link distance between the participating terminals is typically selected to be about or lower than 100 km corresponding to a distance covered by light within the coherence time of the turbulent channel.

Advantageous implementations of embodiments of the present application are the subject of the dependent claims. Preferred embodiments of the present application are described herein below with respect to the figures among which

Fig. 1 shows a block diagram of a key distribution system for providing a cryptographic key to first and second terminals in accordance with an embodiment;

Fig. 2 shows a block diagram of an apparatus for deriving a cryptographic key from refractive-index turbulences as used in the system of Fig. 1 in accordance with an embodiment;

Fig. 3 shows a block diagram of a key generator of the apparatus of Fig. 2 in accordance with an embodiment along with the illustration of signals occurring in the operation of the key generator for illustration purposes;

Fig. 4 shows a block diagram of the system of Fig. 1 with further details for a more precise explanation of the physical processes underlying the key distribution concept in accordance with embodiments of the present application;

Fig. 5 shows a schematic diagram of the external-pupil plane of the key derivation apparatus for illustrating the possibility that receiver's aperture and transmitter's aperture may overlay each other be displaced from other;

Fig. 6 shows a schematic block diagram of a key derivation apparatus in accordance with an embodiment of the present application using a duplexer in the correlation operation of the receiver and the beam shaping operation of the transmitter;

Fig. 7 shows a block diagram of the apparatuses and the system of Figs. 1 to 4 in accordance with an embodiment using the sent-out beams wavefront field as a reference field in the spatial correlation operation;

Fig. 8 shows a block diagram of an embodiment for the apparatuses and the system of Figs. 1 to 4 according to which receiver and transmitter share an SMF so as to have the reference field in the spatial correlation operation adapted to the sent-out beam's wavefront;

Fig. 9 shows a block diagram of a modification of the apparatuses and the system of Fig. 8 according to which separate SMFs are used in receiver and transmitter, both coupled with the turbulence channel via a free-space duplexer; and

Fig. 10 shows a communication system for cryptographic free-space optical communication in accordance with an embodiment.

Fig. 1 shows a system for providing a cryptographic key to first and second terminals, for key distribution or for rendering two identical copies available at the two terminals. The system is generally indicated using reference sign 10, while the terminals are illustrated in Fig. 1 using dashed lines and using reference signs 12 and 14, respectively. The terminals 12 and 14 are separated from each other at a distance L, which may be large such as up to 100 km. Between terminals 12 and 14, a volume 16 filled with gas is present such as the atmosphere, so that turbulences therein cause fluctuations or varying deformations in the phase front of beams traveling therethrough with these fluctuations/deformations being subject to reciprocity.

The system 10 comprises an apparatus for deriving a cryptographic key from turbulences within volume 16 at each terminal 12 and 14, respectively, i.e. an apparatus $18_a$ at terminal 12 and an apparatus $18_b$ at terminal 14. Both apparatuses $18_a$ and $18_b$ may be construed the same or nearly the same way and accordingly, Fig. 2 shows apparatus $18_a$ representatively for both apparatuses $18_a$ and $18_b$. Apparatuses $18_{a,b}$ may be integrated within terminals 12 and 14 or may be separate entities connected with, or being connectable with the same.

Terminals 12 and 14 may, for example, be communication apparatuses implemented as, or being installed onto, mobile or static devices/sites. They may communicate with each other via an optical, electromagnetic or other free-space connection, and use the cryptographic key concurrently provided to both of them by the respective apparatuses $18_a$ and $18_b$ for encryption/decryption purposes. For example, terminals 12 and 14 may use the cryptographic key for OTP encryption/decryption. The communication between apparatuses 12 and 14 may be bidirectional or one-directional. For example, terminals 12 and 14 may be installed at mobile traffic devices such as airplanes, cars, satellites, ships or the like, and/or static devices/sites such as buildings, cranes, skyscrapers, mountains

or the like. As a concrete example, apparatus 12 may be arranged with a static position, while apparatus 14 is, for instance, installed on a moving device.

Fig. 2 shows, representatively for both apparatuses $18_a$ and $18_b$, the internal structure of apparatus $18_a$. As shown in Fig. 2, apparatus $18_a$ comprises a transmitter 20, a receiver 22 and a key generator 24. The transmitter 20 is configured to send out an outbound beam 26 via a first free-space optical channel 28 crossing volume 16 and the receiver 22 is configured to receive an inbound beam 30 via a second free-space optical channel 32 also crossing volume 16, wherein the first and second free-space optical channels are co-aligned, i.e. run exactly along one common line, namely on the same line of sight direction between apparatuses $18_a$ and $18_b$. For co-alignment, transmitter 20 and receiver 22 may interface with channels 28 and 32 via a duplexer a common I/O port of which may redirect, for example, the transmitter's 20 optical axis to a line of sight connection to the other terminal $18_b$ and/or redirect the receiver's optical axis so as to kink from the line of sight connection towards the receiver 22. As shown later with respect to Fig.5, the co-alignment or channel overlay by use of duplexers at apparatuses $18_{a,b}$ is not mandatory. A close parallel extension of both channels may suffice as long as the channel distance obeys some upper threshold such as, for example, defined by the Fried parameter.

In other words, assigned to each other as depicted in Fig. 1, the first free space channel 28 of apparatus $18_a$ coincides with the second free-space channel 32 of apparatus $18_b$ so as to form an interconnecting channel 27a which is subject to reciprocity to the reverse channel 27b corresponding to a coincidence of the second free-space channel 32 of apparatus $18_a$ and the first free-space channel 28 of apparatus $18_b$.

As described in more detail hereinbelow, the key generators of the apparatuses are configured such that they create the (same) cryptographic key based on fluctuations of the transverse optical field of the beam received by the receiver of the respective apparatus after having travelled through volume 16. For example, the receiver measures a spatial correlation between an optical field of the inbound beam 30 and a reference field which coincides with an optical field of the outbound beam 26 and the key generator creates a cryptographic key 36 based on the fluctuations 34 of this spatial correlation. This is done at both apparatuses $18_a$ and $18_b$ in the same way and, thus, owing to the reciprocity, the fluctuations 34 and, accordingly, the created keys at the key generator of both apparatuses $18_a$ and $18_b$ are the same. The "transverse optical field" means the scalar, i.e. irrespective of polarization, complex transverse optical field, i.e. amplitude and phase

at a certain plane such as the external-pupil plane, spatially sampled at points (x,y) within that plane, wherein x,y refer to coordinates of axis spanning the plane.

In particular, in accordance with the embodiments outlined in more detail below, the reciprocity in channels 28 and 32 is obtained by spatial filtering, in amplitude and phase, of the transverse received optical field, i.e. the optical field as entering the receiver, with a filter that corresponds to the transverse optical field of the sent beam, i.e. the optical field as leaving the transmitter of the same apparatus, with this being true at each terminal. Two possible ways of achieving this spatial filtering are described below:

1) One way is to use a single-mode fiber for both the sent beam and the received beam.
2) Another possibility is to use (a part of) the sent beam as a local oscillator for a coherent detection of the received beam.

The reciprocity of the transverse optical fields through the turbulent channel has been theoretically shown in [8] wherein single-mode fibers are used. Polarization is not modified by the atmosphere and thus can be ignored in the reciprocity analysis.

As already described above with respect to Fig. 1, apparatus $18_b$ at the other terminal 14 may be constructed the same way as shown in Fig. 2. When correctly installed so as to result in key distribution system 10 or in correct operation, apparatuses $18_a$ and $18_b$ are oriented towards each other so that the first free-space optical channel 28 of apparatus $18_a$ forms the second free-space optical channel 32 of apparatus $18_b$, or differently speaking, they coincide to form channel 27a, and the second free-space optical channel 32 of apparatus $18_a$ is formed by the first free-space optical channel 28 of apparatus $18_b$, respectively, or differently speaking, both channels coincide to form channel 27b.

The implementation overhead for apparatus $18_a$ (and $18_b$) is low as the outbound beam 26 is supposed to form a one-way signal to pendant apparatus $18_b$, i.e. supposed to travel through volume 16 merely once, with the same being true for the inbound beam 30 which is also merely a one-way signal traveling once through volume 16 from pendant apparatus $18_b$ toward receiver 22 of apparatus $18_a$. That is, no mirror for back-mirroring is necessary, the targeting accuracy is reduced as the effective distance is halved compared to the two-way case, and the problem of how to arrange mirror relative to receive and transmit apertures is omitted.

Fig. 2 illustrates, schematically, the measure F of the spatial correlation between inbound beam 30 and the reference field as a function of time t and illustrates the temporal variation of F over time t which variation is exploited by key generator 24 so as to create the cryptographic key 36.

For example, key generator 24 may perform thresholding of measure F with subsequent sampling so as to obtain m-ary symbols such as bits at some sample rate. That is, the cryptographic key 36 may be a sequence of symbols such as bits and the function used by key generator 24 so as to create the cryptographic key 36 from the fluctuation 34 should be the same for apparatus $18_a$ and $18_b$, respectively. Additionally, this function should be robust against measurement-induced or otherwise occurring deviations in the fluctuations of the spatial correlation measured at the receiver 22 of apparatus $18_a$ and the receiver of apparatus $18_b$, respectively, so that, despite such minor deviations, the same cryptographic key 36 is obtained at both apparatuses $18_a$ and $18_b$. Moreover, it should be noted that the function used to create the cryptographic key 36 from the fluctuations 34 should be adaptive to the mean of the correlation measure so as to be sensitive to the fluctuations thereof, but insensitive to a change in mean power loss, i.e. extinction, of the inbound beam due to, for example, changing weather conditions or the like.

Fig. 3 shows an example for the key generator 24. As shown in Fig. 3, the key generator 24 may comprise a thresholding circuit for subjecting the correlation measure F to thresholding so as to turn the temporal function of measure F into a binary signal x switching between for example two levels $L_1$ and $L_2$ only. The thresholding circuit 38 uses, for instance, two thresholds $F_t^+$ and $F_t^-$ positioned adaptively around a mean $\overline{F}$ of correlation measure F although thresholding circuit 38 may, alternatively, only use one threshold. For instance, thresholding circuit 38 sets signal x to assume level $L_2$ as soon as F exceeds the upper threshold $F_t^+$ and changes the signal x to assume the other level $L_1$ as soon as F succeeds lower threshold $F_t^- < F_t^+$. A digitizer 40, then, turns the analog signal x into a sequence of symbols s(i). To this end, digitizer 40 may apply a constant sample rate so as to sample, for example, the binary signal x at that constant sample rate to obtain binary symbols. Alternatively, digitizer 40 may, for instance, skip, or discard sample values, at sample times of an otherwise constant sample rate which is temporally near to an edge of signal x, i.e. temporally near to times where signal x changes between levels $L_1$ and $L_2$. By this measure, digitizer may leave portions of the signal x where signal x changes its level at times temporally distanced from each other less than a certain

minimum duration $\Delta t$, unsampled so as to increase the robustness of the key creation functionality which is applied equally at the key generator of both apparatuses $18_a$ and $18_b$. The symbol sequence s may, accordingly, be a sequence of bits and key generator 24 may, optionally, additionally comprise an enhancing circuit 42 for enhancing the bit sequence in terms of, for example, inter-bit correlation by, for example, decimating the bit sequence s output by digitizer 40, i.e. reducing its bitrate. For example, enhancer 42 may comprise a feedback shift register (FSR) continuously seeded with the bit sequence s output by digitizer 40, with a readout bitrate for reading out an internal state of the FSR being smaller than the bitrate of the sequence s.

Transmitter 20 and receiver 22 may, for example, be housed in a housing or fixed on a common substrate including or excluding key generator 24 which, in turn, may be embodied as a hardwired circuit, a programmable hardware or as software or a programmed computer. Alternatively, transmitter 20 and receiver 22 may be otherwise be arranged in a fixed position relative to each other. Transmitter 20 and receiver 22 may be coupled to the first and second free-space optical channels 28 and 32 via a duplexer for which examples are set out in more detail below so that channels 28 and 32 overlay each other, namely overlay each other along their way through the medium 16 and at the apparatuses' 18a,b transmitter/receiver's external-pupil planes.

In even other words, and considering the system of Fig. 1 as a whole, the first free-space optical channel 27a via which the apparatus' $18_a$ transmitter 20 of terminal 12 sends beam 26 to the receiver 22 of apparatus $18_b$ of terminal 14 and the second free-space optical channel 27d via which the transmitter 20 of apparatus $18_b$ sends out beam 30 to the receiver 22 of apparatus $18_a$ are subject to reciprocity and, the correlation measured at apparatus 12 and apparatus 14, respectively, are, due to reciprocity, the same. As further described below, transmitter 20 may generate the outbound beam 26 at constant power. However, it should be noted that, alternatively, a predictable change of the sent-out probe beam may be applied as well such as, for example, as a counter-measure against extinction increase due to foggy weather conditions. Power changes of the outbound probe signal are, however, if ever performed at a rate by far slower than the power fluctuations 34. Further, according to the embodiments described further below, the transmitter 20 may use a coherent light source for generating the outbound probe beam. A continuous-wave laser may be used in accordance with the embodiments set-out below, but depending on the circumstances, the transmitter 20 may be implemented using another light source as well.

It should be noted that the spatial correlation is actually a complex-numbered signal, with measure *F* as obtained by the receiver measuring this spatial correlation and resulting in a real-numbered signal which, as described, may then be subject to digitization in generator 24. In other words, the signal digitization is the process of converting the correlation, or measure *F*, from an analog time signal to a bit sequence. The signal digitization typically consists of sampling the signal at regular time intervals and then quantizing the samples using a given number of bits.

Finally, it is noted that the key generator may, for instance, be configured to create the cryptographic key at a bitrate lower than 1 megabit per second or, alternatively speaking, in kHz scale, depending on the speed of the fluctuations 34.

The above description rather generally described embodiments of the present application. The subsequent description provides further explanation in order to assist in understanding the physics underlying the embodiments described herein.

Fig. 4 shows the system of Fig.1 again with, however, additionally showing the internal structure of the apparatuses 18a,b at both terminals 12 and 14. Subscripts a and b are used for distinguishing elements at terminals 12 and 14, respectively. The volume 16 through which beams sent-out by transmitters 22a and 22b travel, is indicated as forming a wavefront-distorting (turbulent) channel 15, namely at the location where the beams travel through volume 16, i.e. where the medium in volume 16 is "probed". The transmitters 20a,b are shown to comprise a light source 48a,b such as a coherent light source. Same may be a laser or even a continuous-wave (CW) laser. A beam shaper 19a,b may, optionally, be comprised as well so as to shape the light source's beam to result in the field 28a,b of outbound beam at the transmitter's aperture 50a,b. As described, apertures 50a and 51a may coincide/overlay each other. Beyond that, transmitter 20a and receiver 22a may also share other components such as a duplexer (cp. 60), a single-mode fiber (cp. 70) which may form the beam shaper 19a of transmitter 20a, an optic at the external-pupil plane (cp. 80) or the like. The same may be said for apparatus 18b.

Due to the distortion, the optical field of the beam sent-out from apparatus 18b and received at apparatus 18a, i.e. the one having travelled from terminal 18b to terminal 18a through volume 16, which is denoted 29a or $E_2^{Rx}$ and represents the complex transverse

optical field received at terminal's 12 apparatus 18a, differs from the optical field of the beam as originally sent-out from apparatus 18b i.e. the one not yet having travelled from terminal 18b to terminal 18a through volume 16, which is denoted 28b or $E_2^{Ref}$. Likewise, the optical field of the beam sent-out from apparatus 18a and received at apparatus 18b, which denoted 29b or $E_1^{Rx}$ and represents the complex transverse optical field received at terminal's 14 apparatus 18b, differs from the optical field of the beam as originally sent-out from apparatus 18a which is denoted 28a or $E_1^{Ref}$.

Each terminal or apparatus has a characteristic property which manifests itself in a reference field. The reference field 23a of apparatus 18a may not be the same as the reference field 23b of apparatus 18b. The reference fields may even vary over time, for example, so as to compensate for changing weather conditions, as indicated above. The reference fields 23a and 23b are discussed in more detail below.

As will be described next with respect to Fig. 7, for example, the sent beam sent out towards the pendant apparatus may be used as a local oscillator for a coherent detection of the received beam, i.e. so as to spatially filter the received transverse optical field $E_{1/2}^{Rx}$ with a filter or reference field 23a,b that corresponds to the (complex scalar) transverse optical field of the sent beam, i.e. $E_{1/2}^{Ref}$, thereby resulting in a measuring of the spatial correlation as mentioned before. Alternatively, as shown in Fig. 8 and 9 in more detail, a single-mode fiber (SMF) may be used for transmission and reception, thereby spatially filtering the received transverse optical field $E_{1/2}^{Rx}$ with a filter or reference field 23a,b that corresponds to the transverse optical field of the sent beam, i.e. $E_{1/2}^{Ref}$. Either the same one SMF may be used as shown in Fig. 8, or SMFs of the same type/construction or having the same fiber mode. In other words, Fig. 4 illustrates that a beam shaper 19a,b such as an optic like a lens or the like or a combination of optics with a SMF, may be present so as to subject the light generated by a light source 48a,b of the transmitter 20a,b to beam shaping so as to result in the transverse optical field of the outbound beam 28a,b, i.e. $E_1^{ref}$, $E_2^{ref}$ i.e. at the external-pupil plane. As just-mentioned, this field may be co-used as the reference field in the reception by the receiver as shown in Fig. 7, or the receiver uses optical structure for achieving a spatial filtering of the inbound beam which substantially coincides with the filtering of beam shaper 19a,b as shown in Fig. 8 and 9. For example, the receiver 22 receives the inbound beam via an SMF of the same type as shown in Fig. 9 or even the same SMF as the one of transmitter 20 as shown in Fig. 8.

The receiver's 17a,b operation of measuring the spatial correlation between the received field 29a and the transmitted reference field 28a requires, so as to be performed without approximation, a spatial overlap of 28a and 29a. An approximation may, however, suffice. See for example, Fig. 5. In particular, a spatial overlap of the incoming and outgoing beams in the terminal's external plane may not be necessary if the correlation width of the received field 29a is much larger than the transverse separation $d$ between the Tx and Rx apertures 50, 51 of the terminal, i.e. between the aperture 51 of the receiver and the aperture 50 of the transmitter of the respective apparatus. As an example the correlation width of the received field 29a can be described as the Fried parameter [9] and noted $r_0$. Fig. 5 shows the external-pupil plane 49a of the terminal 18a where the transmitting aperture 50 of transmitter 22a and the receiving aperture 51 of receiver 22a are separated by a distance $d$ . The random received field 29a can be characterized by the Fried parameter $r_0$. If the aperture separation is much smaller than the Fried parameter (i.e., $d << r_0$), then the receiver's 22a correlation measuring operation can be performed to a good approximation and secret key distribution is possible as described assuming channel overlay. Fig. 6 illustrates that, if a spatial overlap of 28a and 29a (respectively, 28b and 29b) is used, a duplexer 60a (respectively 60b) may be present in apparatus 18a (respectively 18b), which is used to spatially separate the incoming and outgoing beams of the single optical antenna or external aperture.

As shown in Fig. 6 a duplexer 60 can be included in the terminal. In that case, the beam shaping 19a and the correlation operation performed by the receiver 22a which is indicated by 17a have duplexer 60 in common.

That is, as outlined further below, the transmitter 20a or its transmitting path, which includes the transmitter's 20a light source and the beam shaper 19a, and the receiver 22a or its receiving path, which includes the receiver's 22a components which perform the correlation operation 17a, may have common optics including duplexer 60 and, optionally, other optics (not shown in Fig. 7). A common I/O port (the overlay of 50 and 51) of the duplexer 60 redirects the optical axis of the beam shaper 19a to a line-of-sight connection to the other terminal 18b and redirects the receiver's optical axis so as to kink from the line-of-sight connection towards the correlation operation apparatus 19a.

With respect to Fig. 7-9, the embodiments described above are described in more detail. In other words, Fig. 7 to 9 form examples for implementing the system and apparatuses shown in Fig. 1 to 6.

In Fig. 7, the arrows 8a and 9a (respectively 8b and 9b) both represent the reference field 23a (respectively 23b) of Fig. 4 although they have different polarizations. In Fig. 7, the receiver 22a comprises an optical coherent-detection receiver 63a arranged between key generator on the one hand and duplexer 60a on the other hand. Duplexer 60a is here embodied as a polarization sensitive free-space beam splitter, an IO port of which forms the overlay of apertures 50a and 51a. The duplexer 60a is co-owned by receiver 22a and transmitter 20a. Transmitter 20a comprises, beyond laser 48a and a polarizer 61a positioned downstream laser 48a and assuming the task of individualizing the laser's beam so as to be distinguishable from the inbound beam of the other apparatus 18b for duplexer 60a, a beam splitter 62a for providing the optical coherent-detection receiver 63a with a copy of the polarized beam 3 having been individualized by polarizer 61a, a mirror 65a, a polarization rotator such as a half-wave plate 64a and the duplexer 60a, which are in the order of their mentioning, positioned downstream optics 61a. Mirror 65a redirects the portion of beam 3 having passed beam splitter 62a via polarization rotator 64a to a first port of duplexer 60a, which in turn redirects the polarization rotated beam 8a towards terminal B as the outbound beam 2a. Optical coherent detection receiver 63a receives both the portion 9a copied from beam 3 by beam splitter 62a as well the inbound beam 43a via duplexer 60a, namely the inbound beam 1a having traveled from the IO port of duplexer 60a towards another port of duplexer 60a. The optical coherent-detection receiver 63a may use a beam splitter so as to overlay beam 9a with beam 1a, detect the overall beam power by use of a photodetector, and forward the measured analog signal to key generator 24a for the key generation process involving the signal digitization as described previously. As terminal 14 and apparatus 18b are constructed nearly – see the optional differences concerning duplexing - the same way, the description just brought forward pertains to apparatus 18b in the same manner.

The correlation operation 17a is here represented by the following parts: the optical coherent-detection receiver 63a, the propagating fields 9a and 43a, the polarization-independent beam splitter 62a and the polarization beam splitter 60a. The coherent detection in receiver 63a typically delivers the following output signal:

$$\iint \left| E_1^{ref*}(x,y) + E_2^{Rx}(x,y) \right|^2 dxdy = \iint \left| E_1^{ref}(x,y) \right|^2 dxdy + \iint \left| E_2^{Rx}(x,y) \right|^2 dxdy + 2\,\mathrm{Re} \overbrace{\iint E_1^{ref}(x,y) E_2^{Rx}(x,y) dxdy}^{spatial\ correlation}$$

where the terms $\iint \left| E_1^{ref}(x,y) \right|^2 dxdy$ and $\iint \left| E_2^{Rx}(x,y) \right|^2 dxdy$ can be filtered out, leaving the real part of the correlation term. Thus the function $F_0()$ from the operation 17a in receiver 22a, and 17b in receiver 22b, consists mainly in taking the real part of the correlation. As shown in Fig. 5, x,y denote the transverse coordinates.

The beam shaping 19a is represented in Fig. 7 primarily by internal parts of the transmitter's source 48a so that both, reference field and outbound field are spatially shaped equally. The complex scalar transverse reference field 23a, and of the outbound beam, respectively, can be relatively arbitrarily chosen.

The duplexer 60a according to Fig. 6 is here implemented as a polarization beam splitter.

The two input beams 9a and 43a (respectively 9b and 43b) of coherent detection 63 in Terminal A (respectively Terminal B) should have equal polarization. This equal polarization is guaranteed by the polarizer 61a,b which is identical in both terminals and the half-wave plates 64a and 64b. The polarizer 61a,b which for example polarizes the light linearly in the vertical direction.

Beams 8a and 43a (respectively 8b and 43b) in Terminal A (respectively Terminal B) have orthogonal polarization states and thus can be combined/separated by the polarization beam splitter 60a,b.

Any optics may be placed between the beam splitter 60a,b and the external-pupil fields 1a and 2a.

As already described above with respect to Fig. 1 to 4, and as shown in Fig. 7 to 9, apparatuses 18a and 18b may be constructed in a similar way.

Apparatuses 18a,b in Terminal A and Terminal B in Fig. 8 can be substantially the same. We thus focus on the description of apparatus 18a in Terminal A. In Fig. 8, the receiver 22a comprises, along the direction from the overlay of apertures 50a and 51a on, an optic or lens 80a, a single mode fiber (SMF) 70a, one end of which is positioned at the focus of optic or lens 80a, a single mode fiber duplexer 60a and a photodetector 71a connected to a port of duplexer 60a via an SMF 72a, with the duplexer 60a being configured to copy light received via SMF 70a after traveling through volume 16 via SMF 72a to photodetector 71a. Transmitter 22a comprises a CW laser 48a as light source, which couples its generated light via an SMF 73a to another port of duplexer 60a. SMF 70a and optic or lens 80a also belong to transmitter 20a, i.e. they are shared by receiver and transmitter. The duplexer 60a is configured to couple light received from laser 48a via SMF 73a into SMF 70a so as to be sent-out as the outbound beam. The construction of the apparatus 18b at the other terminal B is the same but with a reversal of the beams' duplexing property (e.g. polarization, wavelength, direction).

The duplexer 60a according to Fig. 6 is here implemented as a single-mode fiber duplexer 60.

The arrows 1a and 2a (respectively 1b and 2b) both represent the reference field 23a (respectively 23b).

The correlation operation 17a or 17b is here represented by the following parts: photodetector 71a, the single-mode fiber 72a from the duplexer 60a to the photodetector 71a, the single-mode fiber duplexer 60a, the single-mode fiber 70a from the optics 80a to the duplexer 60a, the optics 80a. The photodetected signal is proportional to the term

$$\left| \overbrace{\iint E_1^{ref}(x,y)\, E_2^{Rx}(x,y)\, dxdy}^{spatial\ correlation} \right|^2 .$$

Thus the function $F_0()$ from the operation 17a and 17b consists mainly in taking the squared modulus of the correlation. Please note that here $E_1^{ref}$ is a result of the spatial filtering induced by the SMF and the projection performed by the optics 80a und is, thus, related to the SMF's impulse response of the SMF's mode. $E_2^{Rx}$ is, as denoted above, the complex scalar optical field of the inbound beam 1a at the receiver's aperture, and the integration and modulus is a result of the operation of the photodetector.

The beam shaping 19a is in Fig. 8 primarily achieved by the single-mode fiber 70a from the optics 80a to the duplexer 60a, and the optics 80a itself which are both part of the transmitter's and the receiver's optical path so that the reference field achieving the spatial correlation and the field of the outbound beam coincide.

The light source 48a is here embodied as continuous-wave (CW) laser. The laser has a constant output power because its field should correspond to the terminal's reference field which is determined by the fundamental mode of the SMF and which does not vary in time.

Changes can be applied to the reference field. Therefore the same changes can be applied to both the outbound beam and to the spatial filtering of the received beam. These changes are implemented, for example, as a damper arranged within the transmitter's and receiver's common optical path so as to reciprocally damp the outbound and inbound beams power at one of both apparatuses 18a,b so as to vary or modulate or adjust the power for any reason. As the variation affects the correlation in both apparatus 18a and apparatus 18b, namely in form of the inbound beam in the other (non-varying apparatus) and the outbound beam (actively varying apparatus) respectively, the correlation remains equal in both apparatuses 18a,b and so do the derived (distributed) keys.

Changes applied only to the source power 48a are possible if they are predictable or can be disassociated from the key signal. For example, at a rate by far slower than the fluctuations of the correlation signal, the power of source 48a may be changed so as to, for example, compensate for changing weather conditions.

The front optics 80a and 80b may not be the same.
The front optics 80a and 80b are typically collimating lenses of diameter 0.5 to 10 cm.
The optics represented by 80a and 80b is here drawn as a collimating lens but can be any optics, including adaptive optics, or it can be left off completely in other embodiments. Note that if 80a includes adaptive optics then the reference field 23a varies in time.

As shown in Fig. 8, the light source 48a (respectively 48b) may be embodied as a continuous wave (CW) laser.

The transmit and receive paths interface with the free-space channel 16 via a common single-mode fiber 70a a fiber end of which is positioned at a focus of a collimator 80a.

As the photodetector 71 merely measures the power fluctuations, the optical instruction is kept easy. No longitudinal-phase comparison between the fields 1a and 2a needs to be performed. In other words, no mixing between the fields 1a and 2a is necessary prior to photodetection. The inbound probe signal 2a may be routed onto a photodetector such as a photo diode or the like.

The terminal's reference field 23a is shaped by the fundamental mode of the deployed SMF 70a. The collimator 80a serves to reduce beam enlargement of the sent-out probe signals. The SMFs 70a, 72a, 12a shown in Fig. 8 may be standard SMFs, i.e. they do not have to be polarization-maintaining.

The duplexing can be, for example, performed over the propagation direction, the wavelength or the polarization.

In any case, the duplexer 60 directs, via single-mode fiber 72a, the signal from bidirectional fiber 70a to the photodetector 71, and directs, via single mode fiber 73a, the signal from the light source 48a to the bidirectional fiber 70a.

For duplexing with signal division over the propagation direction, the duplexer 60 can be embodied as a circulator. Note that, in this duplexing case, apparatuses 18a and 18b can be exactly the same, i.e. equal in the components used, in the inter-component arrangement and in their operational parameters (e.g., wavelength, polarization). Terminals deployed for several links can then be identical and compatible with each other, allowing an easy re-use of the terminals and a quick reconfiguration of the links. However, as described in the above embodiments using other duplexing techniques, the terminals 18a and 18b may slightly differ from each other for duplexing purposes. That is, the division parameter such as wavelength or polarization of the emitted beam, may be transposed from one terminal to the other. Thus, in that case, the terminals may equal in the components used, but differ in inter-component arrangement such as rotational state of a polarizer, or in operational parameter of a component such as the transmitter's wavelength.

For polarization-division duplexing, the duplexer 60 can be embodied as a fiber-based polarization beam splitter.

Fig. 9 shows a modification of Fig. 8. In particular, in accordance with Fig. 9 receiver 22a and transmitter 20a use separate pairs of SMF 75a (receiver) and 76a (transmitter) in combination with a respective optic or lens 81a (receiver) and 82a (transmitter), respectively, in order to separately receive and transmit light to and from duplexer 60a, which here is embodied as a free-space beam splitter. With the SMFs 75a and 76a and associated optics 81a and 82a being of the same type, the spatial filtering involved in the correlation measurement by the receiver 22a corresponds to the spatial filtering imposed onto the outbound beam sent out by transmitter 20a just as is the case in Fig. 8, where one SMF has been commonly used by receiver and transmitter, respectively.

In both embodiments in Fig. 8 and Fig. 9, for wavelength-division duplexing, the duplexer 60a can alternatively be embodied as a wavelength de-/multiplexer (e.g. arrayed waveguide grating). For wavelength-division duplexing, the light sources 48a and 48b of both apparatuses 18a and 18b send out their probe signals with a different wavelength $\lambda_1$ and $\lambda_2$ with $\lambda_1 \neq \lambda_2$. The wavelengths should be close enough to each other to provide substantially identical turbulence-induced perturbations. For example, $2 \cdot |\lambda_1 - \lambda_2| / (\lambda_1 + \lambda_2)$ is smaller than 5%. Thus, in case of Fig. 8 and Fig. 9, a dichroic beam splitter 60a (respectively 60b) would supply the detector 71a (respectively 71b) with a beam emitted by apparatus 18b (respectively apparatus 18a).

The arrows 1a and 2a (respectively 1b and 2b) both represent the reference field 23a (respectively 23b) of Fig. 4.

The correlation operation performed by the receiver 22a of Fig. 4 is, in Fig. 8, represented by photodetector 71a, the single-mode fiber 70a, and the optics 80a, and in Fig. 9 by photodetector 71a, the single-mode fiber 75a, and the optics 81a.

The beam shaping 19 of Fig. 4 is, in Fig. 8, primarily represented by the single-mode fiber 70a, and the optics 80a and in case of Fig. 9, where the duplexer 60 is implemented as a free-space beam splitter, by the single-mode fiber 76a and optics 82a.

Incoming beam and outgoing beam can be separated for example over the wavelength, in which case beam splitter 60a could be a dichroic beam splitter. Duplexing can also for example be performed over polarization in which case beam splitter 60a could be a polarization beam splitter.

The transmit path and the receive path should be precisely co-aligned and should perform substantially the same optical processing of the complex scalar transverse field.

The SMF can be replaced by any filtering device that would provide a reference transverse field $E_{ref}(x,y)$ that is used both as a transmitted optical field and as a spatial filter to the received field prior to detection. Again, this filtering device may not be the same at apparatus 18a and apparatus 18b.

One terminal described in Fig. 8 (respectively Fig. 9) may form a key distribution link with a terminal described in Fig. 9 (respectively Fig. 8) provided that the two terminals have compatible duplexing schemes.

Thus, the above embodiments revealed a relatively cheap possibility to distribute, in a secret manner, a key over a turbulent optical channel. In particular, a single coupling optics (or optical antenna) suffices at each terminal. Moreover, the key distribution concept outlined above offers a highly secure method by exploiting the fact that the spatial correlation of the two emitted beams in a given transverse plane between Terminal A and Terminal B cannot be calculated without deploying extraordinary efforts. In practice, the key can be measured only at the position of Terminal A or Terminal B. A possible application may look as follows. The concepts outlined above may be used, for instance, for a secure communication in cities between any two buildings which are closer than 100 km, for example, as long as the line of sight is not blocked. Therefore, the above concept could be used, for example, on high buildings or buildings located at higher places, with a Terminal A being positioned at one such building, and a Terminal B being positioned at another building, for example. The above concept could also be used in relation to mobile terminals 18a and 18b. Imagine, for example, a scenario where fiber-based communication is not an option such as in case of cars, ships and airplane. With a terminal 18a or 18b on a fast aircraft, the channel changes faster than when the beam axis is static through the air. Fast channel changes induce fast signal fluctuations which in turn allow high bitrates compared to stationary terminals.

In the above embodiments, optical propagation through a turbulent volume such as a turbulent atmosphere has been exploited for key distribution. For the purpose of reciprocity, substantially identical wavelengths have been used for the exchanged (transmitted and received) beams. The wavelength may, for instance, be closer than ±

5%. For optimal reciprocity of the bidirectional link, a common optics for the transmitted and received beams were used. The key signal finally results from a function applied on the spatial correlation between the emitted and received beams.

This analog signal derived from the correlation was calculated in different ways, i.e. with different embodiments described above. One embodiment version uses the superposition of the emitted and received beams leading to an optical coherent detection. Other versions deploy fibers as a way to create a reference transverse field used both as the transmitted optical field and as a spatial filter to the received field prior to photodetection. The simplest type of fiber that produces a deterministic filtering of the scalar (i.e. without polarization information) transverse field is the standard single-mode fiber.

For the sake of completeness, Fig. 10 shows a system for cryptographic free-space optical communication comprising a system according to Fig. 1 which may be modified or implemented in accordance with any of the details described above with respect to Figs. 2-6. The system of Fig. 10 is generally indicated using reference sign 70. It comprises the first terminal device 12 and the second terminal device 14 in addition to the apparatus $18_a$, the first terminal device 12 comprises a message encryptor configured to encrypt a message using a cryptographic key 36 as obtained by apparatus $18_a$ and a message transmitter 74 configured to transmit the encrypted message 76 to terminal device 14 which, in turn, in addition to apparatus $18_b$ comprises a message receiver configured to receive the encrypted message 76 and a message decryptor 78 configured to decrypt the encrypted message 76 using the cryptographic key forwarded by apparatus $18_b$. The message encryptor 72 may receive the message to be encrypted via an input 80 while message decryptor 78 may output the decrypted message via an output 82. A symmetric en/decryption scheme may be used be message en/decryptors 74 and 78, respectively, such as OTP en/decryption using, for example, a bitwise XORing between cryptographic key and plain/encrypted message, respectively.

Thus, insofar, terminal 12 of Fig. 10 represents a sender for encrypted free-space optical communication while terminal 14 acts as a receiver for encrypted free-space optical communication. A bidirectional communication may, however, also take place so that each of terminals 12 and 14 act both as receiver and sender, i.e. communication transceivers. In that case, message receiver and message decryptor would also be present in terminal 12 with corresponding message transmitter and message encryptor being present at terminal 14.

The transmission between message transmitter 74 and message receiver 76 may, preferably, take place wirelessly using, for example, electromagnetic transmission, optical transmission or some other sort of free-space transmission. Separate transmitter and receiver may be present to this end at terminal 12 and 14, respectively, in addition to those of apparatuses $18_a$ and $18_b$. In case of optical message transceivers, same may be operated using a shared-optics operation as well, with using, however, separate reciprocal channels.

Message encryptor 72 may use OTP encryption so as to encrypt on original message 80 using the cryptographic key 36 and message decryptor 78 may use OTP decryption, accordingly, thereby resulting in an encrypted message 76. The OTP encryption/decryption may, for example, be implemented by XORing each bit of message 80/76 with a respective bit of the cryptographic key 36. Accordingly, the bitrate of the cryptographic key 36 would coincide with a message bitrate at which message 76 is transmitted between terminals 12 and 14, respectively. Alternatively, each bit of the cryptographic key 36 may be used to encrypt a greater portion of message 80/76 for example, i.e. a portion longer than one bit. For example, the cryptographic key 36 available at both terminals 12 and 14 may be used to form keys of block ciphers/deciphers within encryptor/decryptor 72/78 in a manner so that a sequence of keys equally derived from the key generators at both apparatuses $18_a$ and $18_b$ is used for en/decrypting a sequence of blocks of message. Alternatives are feasible as well.

References

1. Bennett, Charles H „ and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Vol. 175. No. 0. 1984

2. Kravtsov, Konstantin, et al "Physical layer secret key generation for fiber-optical networks " Optics express 21.20 (2013) : 23756-23771 .

3. Drake, Marvin D , et al. "Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance" Optical Engineering 52 5 (2013);055008-055008 .

4 US20100080386 A1

5. Hershey, John E.„ Amer A. Hassan, and Rao Yarlagadda. "Unconventional cryptographic keying variable management " Communications, IEEE Transactions on 43 1 (1995): 3-6

6. Aono , Tomoyuki, et al. "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels." Antennas and Propagation, IEEE Transactions on 53 11 (2005) : 3776-3784 .

7. Mathur, Suhas, et al. "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel " Proceedings of the 14th ACM international conference on Mobile computing and networking ACM, 2008.

8. Shapiro , Jeffrey H , and Andrew L. Puryear "Reciprocity-enhanced optical communication through atmospheric turbulence---Part 1: Reciprocity proofs and far-field power transfer optimization " Journal of Optical Communications and Networking 4 12 (2012 ): 947-954 .

9. Fried, D., "Optical Resolution Through a Randomly Inhomogeneous Medium for Very Long and Very Short Exposures," J. Opt. Soc. Am. 56, 1372–1379 (1966)

Claims

1. Apparatus for deriving a cryptographic key, comprising:

a optical transmitter (20) configured to send out an outbound beam (26) through a random wavefront-distorting medium to an external terminal;

a receiver (22) configured to receive an inbound beam (30) through the random wavefront-distorting medium from the external terminal and to provide a measure of a spatial correlation between a transverse optical field of the inbound probe beam and a reference field which coincides with a transverse optical field of the outbound beam; and

a key generator (24) configured to create a cryptographic key (36) based on the fluctuations of the measure of the spatial correlation (34).

2. Apparatus according to claim 1, wherein the transmitter (20) and the receiver (22) perform the send-out and reception commonly via a duplexer so that the outbound beam and the inbound beam overlay each other in an external-pupil plane.

3. Apparatus according to claim 1 or 2, wherein the transmitter comprises a coherent light source configured to generate a source beam and a beam shaper configured to spatially shape the source beam so as to obtain a shaped source beam, and the receiver is configured to superpose the shaped source beam and the inbound beam and measure the power of the superposed fields.

4. Apparatus according to any of the previous claims, wherein the transmitter is configured to send-out the outbound beam and the receiver is configured to measure a power of the inbound beam via a single-mode fiber, respectively, so that a beam shaping of the outbound beam and a spatial filtering of the inbound beam before the measurement of the power thereof, resulting from the single-mode fiber, respectively, coincide.

5. Apparatus according to any of the previous claims, further comprising a duplexer and a single-mode fiber, wherein the duplexer interfaces the transmitter and the

receiver with the single-mode fiber so that, via the single-mode fiber, the transmitter sends out the outbound beam and the receiver receives the inbound beam.

6. Apparatus according to claim 5, wherein the duplexer is a single-mode fiber duplexer or a free-space duplexer.

7. Apparatus according to any of the previous claims, wherein the transmitter comprises a continuous-wave laser.

8. Apparatus according to any of the previous claims, wherein the key generator (24) is configured to create the cryptographic key by way of digitization.

9. Key distribution system for providing a cryptographic key to first and second terminals, the key distribution system comprising

a first apparatus for deriving a cryptographic key at the first terminal, comprising

a transmitter (20) configured to send out a first beam (26) through a random wavefront-distorting medium;

a receiver (22) configured to receive a second beam (30) through the random wavefront-distorting medium; and

a key generator (24) configured to create a cryptographic key (36) based on fluctuations (34) of a transverse optical field of the second beam (30) received by the receiver of the first apparatus; and

a second apparatus for deriving the cryptographic key at the second terminal, comprising

a transmitter (20) configured to send out the second beam (30) through the random wavefront-distorting medium;

a receiver (22) configured to receive the first beam (26) through the random wavefront-distorting medium; and

a key generator (24) configured to create the cryptographic key (36) based on fluctuations (34) of a transverse optical field of the first beam (26) received by the receiver of the second apparatus.

10. Key distribution system according to claim 9, wherein the first and second apparatuses are identical in components used in construction, with differences, if ever, lying in inter-component arrangement and/or components' operational parameters.

11. Key distribution system according to claim 9 or 10, wherein the first and second apparatuses are formed by an apparatus according to one of claims 1 to 8, respectively.

12. Communication system for cryptographic free-space optical communication comprising a first terminal device (12) and a second terminal device (14), wherein the first terminal device (12) comprises a message encryptor (72) configured to encrypt a message using a cryptographic key (36) and a message transmitter (74) configured to transmit the message (76) to the second terminal device (14) and the second terminal device (14) comprises a message receiver (76) configured to receive the message from the first terminal device (12) and a message decryptor (78) configured to decrypt the message using the cryptographic key (36), wherein the communication system comprises a key distribution system according to any of claims 9 to 11.

13. Sender for encrypted free-space optical communication, comprising:

an apparatus for deriving a cryptographic key according to any of claim 1 to 8;

a message encryptor configured to encrypt a message using the cryptographic key; and

a message transmitter configured to transmit the encrypted message.

14. Receiver for encrypted free-space optical communication, comprising:

a message receiver configured to receive a message;

an apparatus for deriving a cryptographic key according to any of claims 1 to 8; and

a message decryptor configured to decrypt the message received using the cryptographic key.

15. Method for deriving a cryptographic key, comprising:

sending out an outbound beam (26) through random wavefront-distorting medium to an external terminal;

receiving an inbound beam (30) through the random wavefront-distorting medium from the external terminal with providing a measure of a spatial correlation between a transverse optical field of the inbound probe beam and a reference field which coincides with a transverse optical field of the outbound beam; and

creating a cryptographic key (36) based on the fluctuations of the measure of the spatial correlation (34).

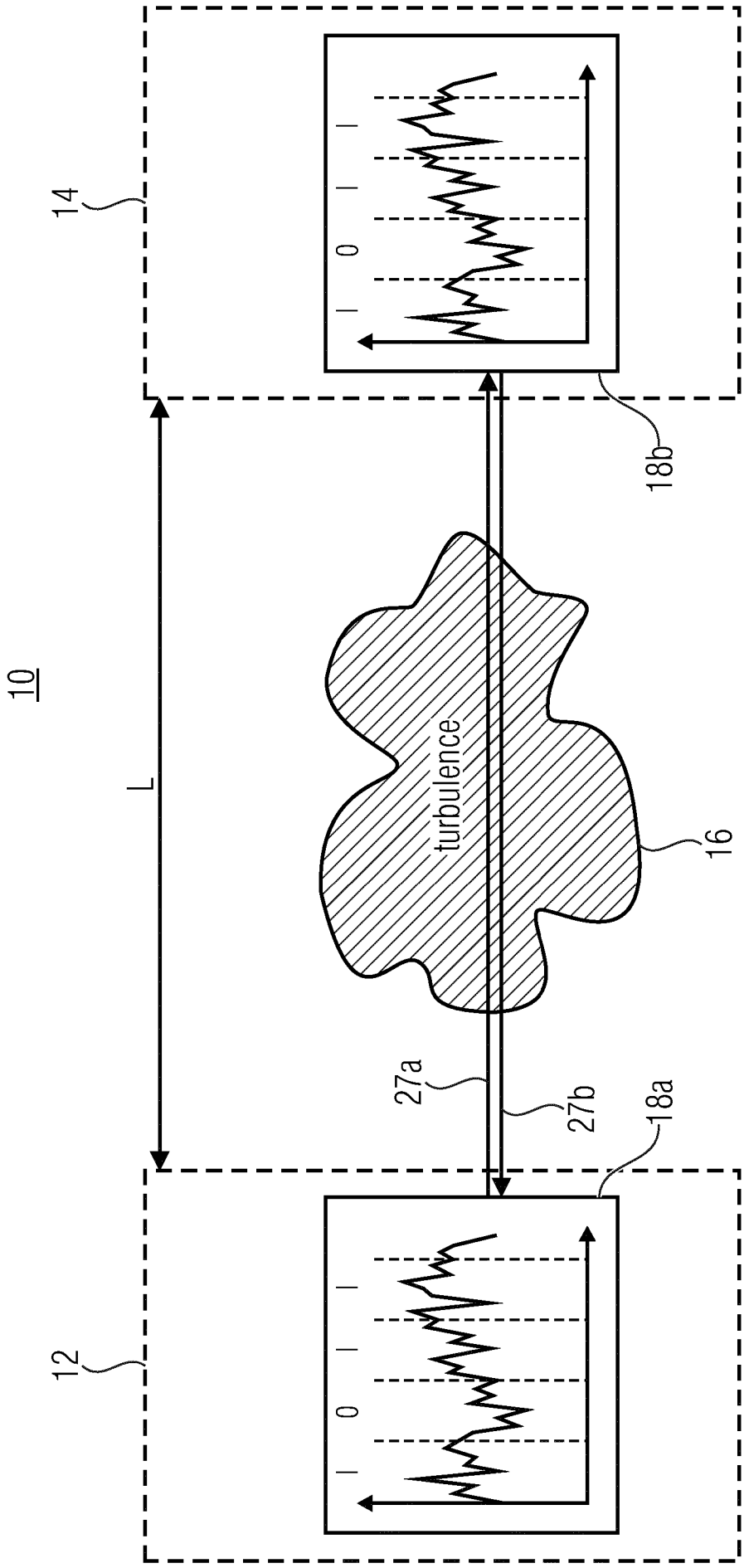


FIG 1

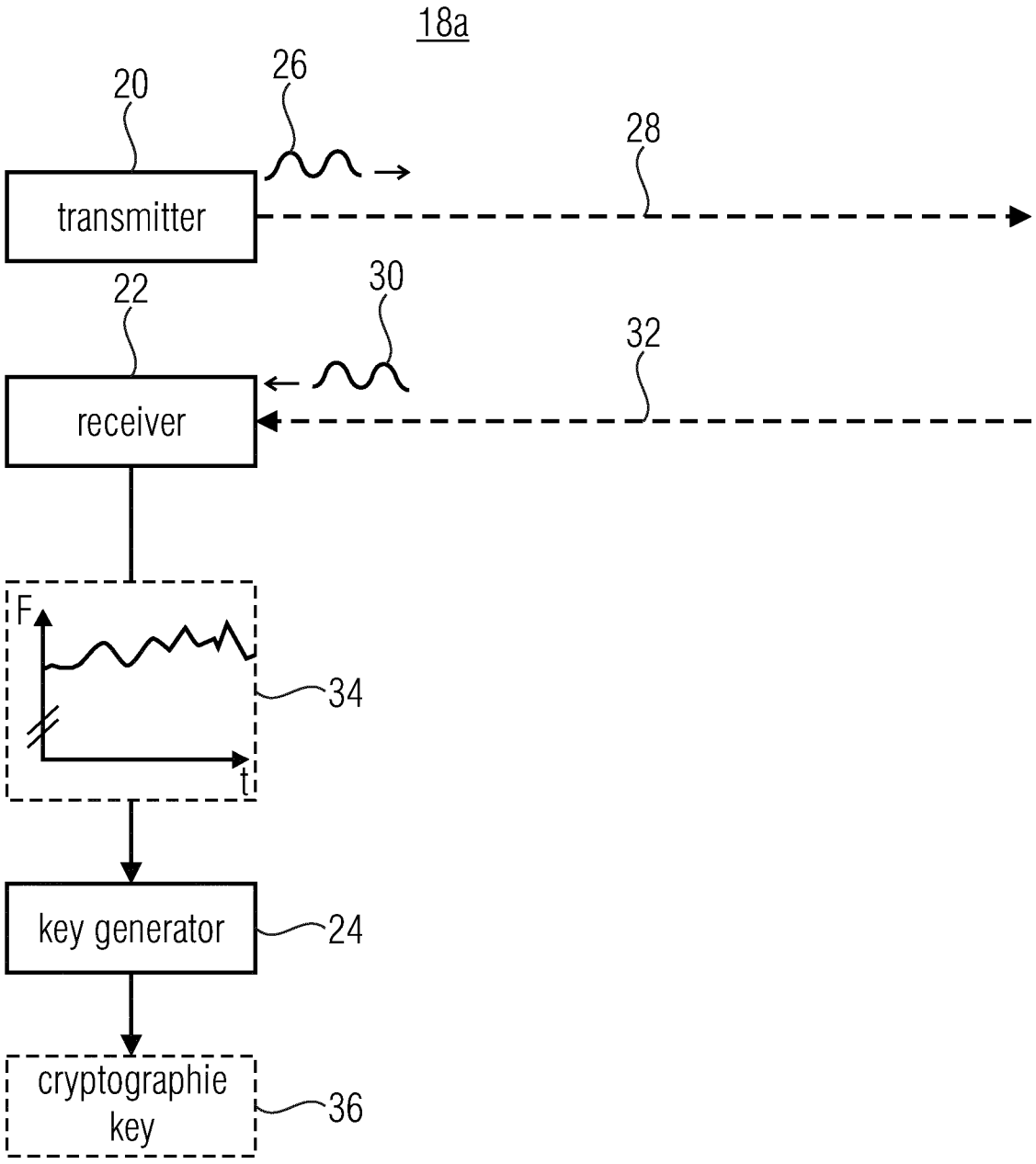
18a
20
26
28
transmitter
22
30
32
receiver
F
t
34
key generator
24
cryptographie key
36

FIG 2

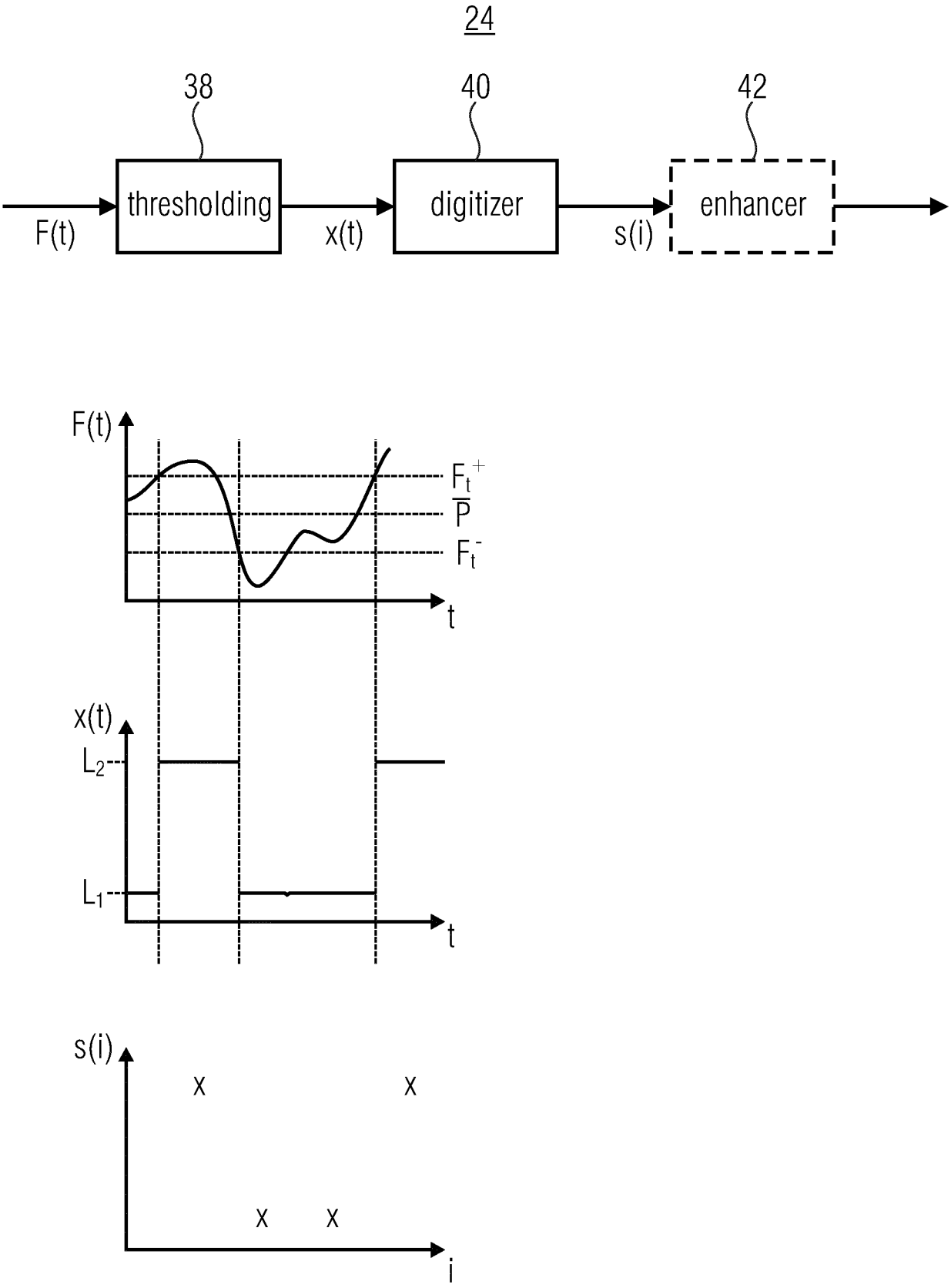
24
38
40
42
thresholding
digitizer
enhancer
F(t)
x(t)
s(i)
F(t)
$F_t^+$
$\overline{P}$
$F_t^-$
t
x(t)
$L_2$
$L_1$
t
s(i)
x
x
x
x
i

FIG 3

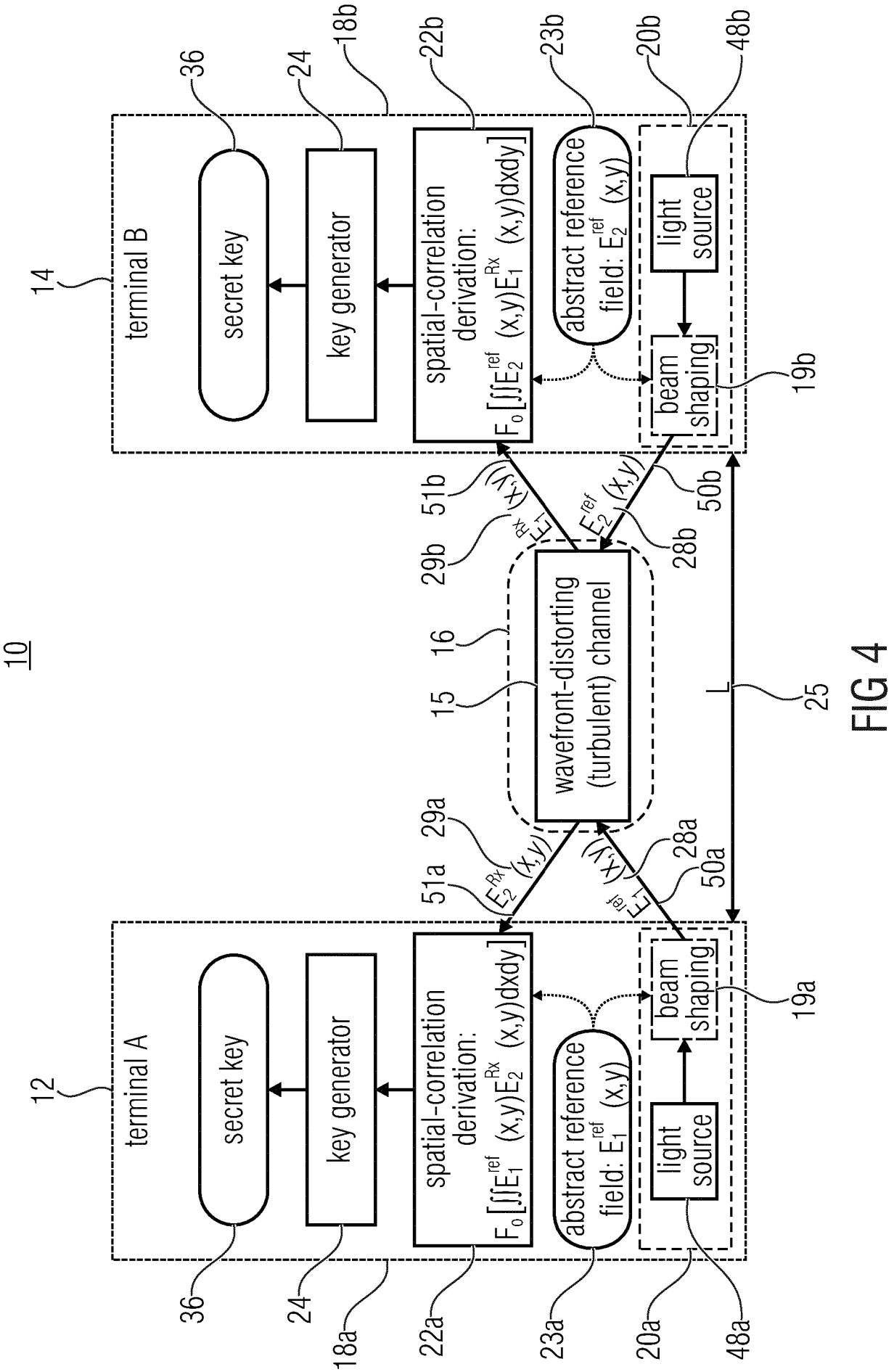
10
12
terminal A
secret key
key generator
spatial-correlation derivation:
$F_0[\int\int E_1^{ref}(x,y)E_2^{Rx}(x,y)dxdy]$
abstract reference field: $E_1^{ref}(x,y)$
light source
beam shaping
14
terminal B
secret key
key generator
spatial-correlation derivation:
$F_0[\int\int E_1^{ref}(x,y)E_2^{Rx}(x,y)dxdy]$
abstract reference field: $E_2^{ref}(x,y)$
light source
beam shaping
wavefront-distorting (turbulent) channel
15
16
L
25
$E_2^{Rx}(x,y)$
$E_1^{ref}(x,y)$
$E_2^{ref}(x,y)$
$E_1^{Rx}(x,y)$
18a
18b
19a
19b
20a
20b
22a
22b
23a
23b
24
24
28a
28b
29a
29b
36
36
48a
48b
50a
50b
51a
51b

FIG 4

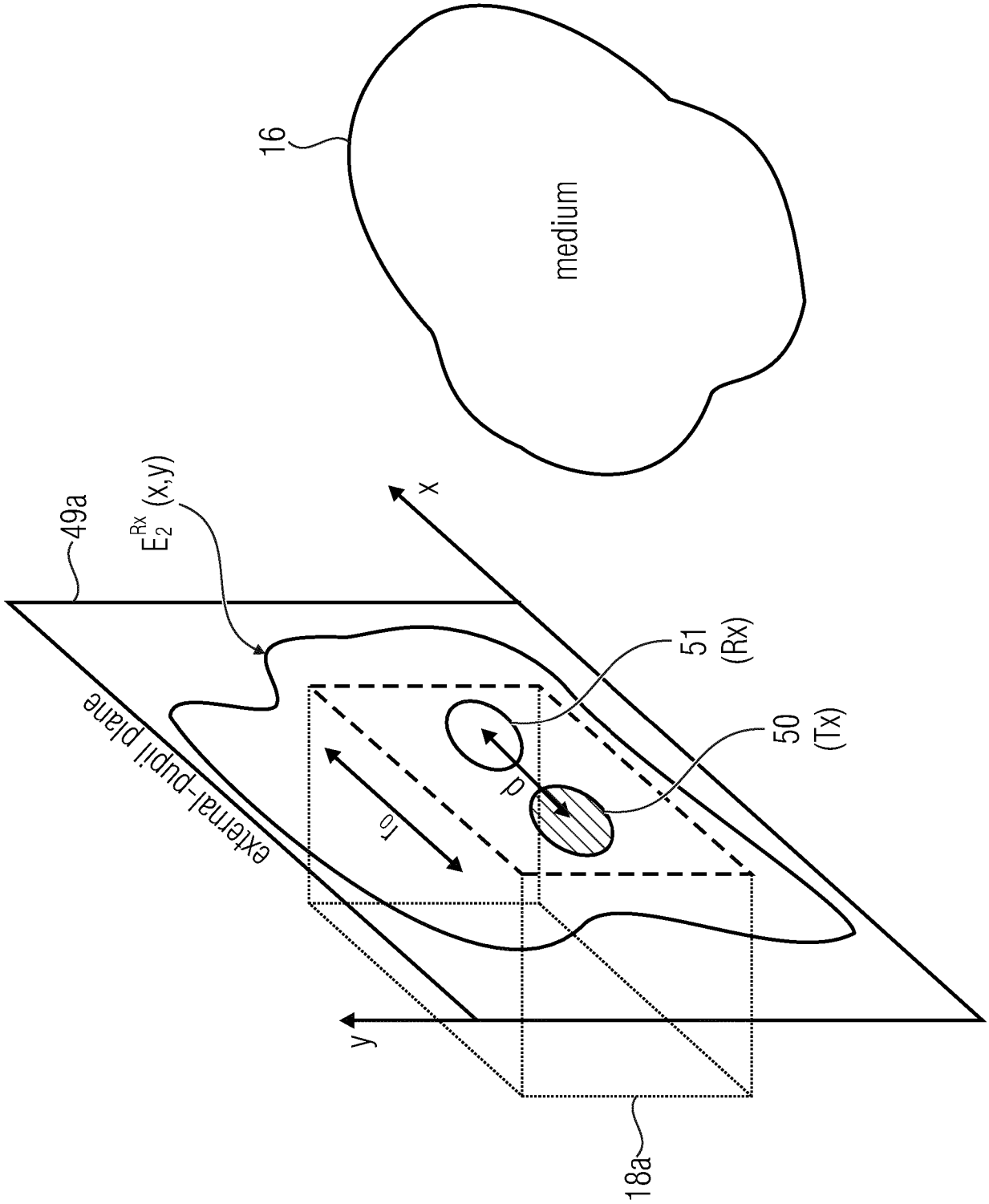
16
medium
49a
$E_2^{Rx}(x,y)$
x
51
(Rx)
50
(Tx)
d
$l_0$
external-pupil plane
y
18a

FIG 5

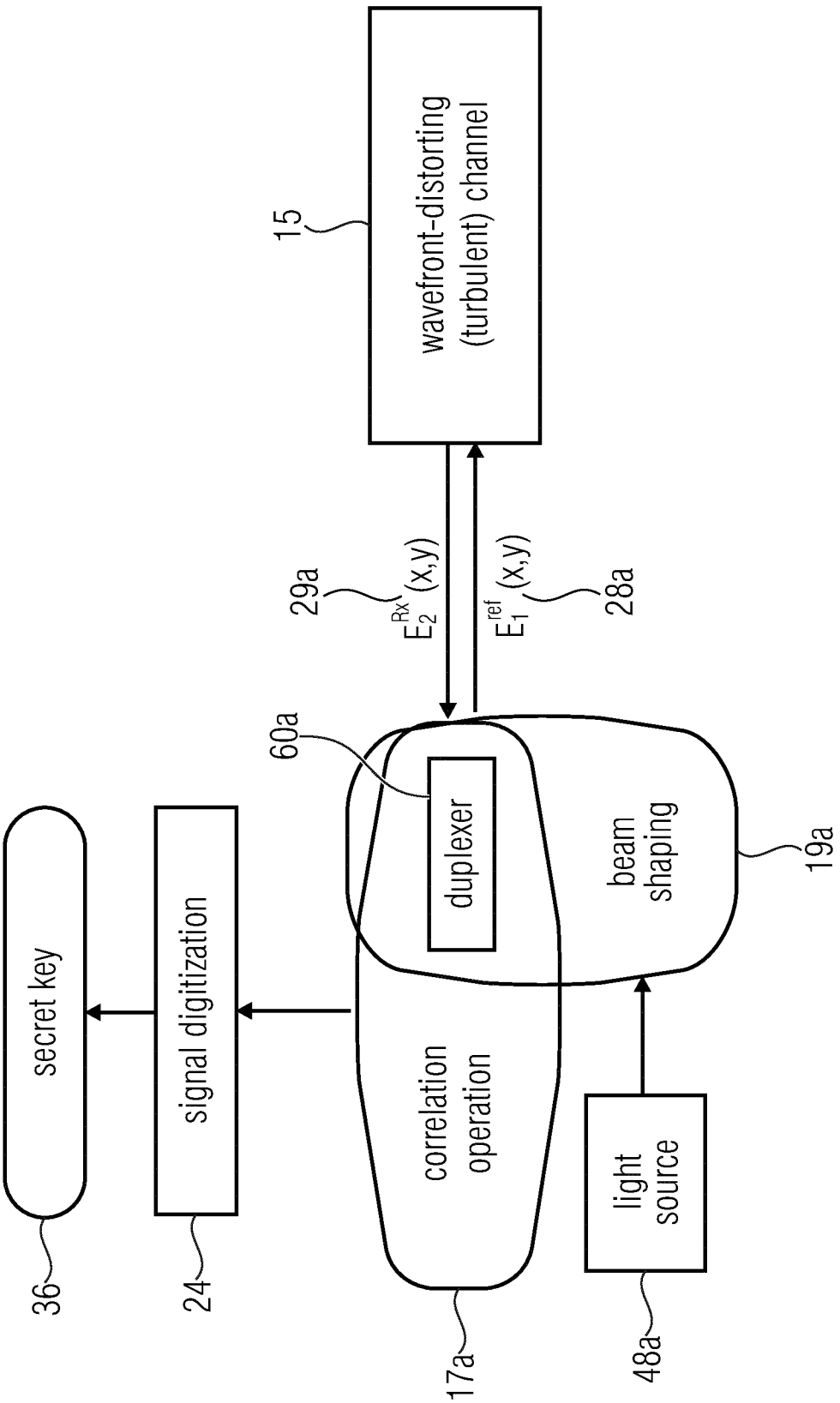
wavefront-distorting (turbulent) channel
15
29a
$E_2^{Rx}(x,y)$
$E_1^{ref}(x,y)$
28a
60a
duplexer
beam shaping
19a
secret key
signal digitization
correlation operation
light source
36
24
17a
48a

FIG 6

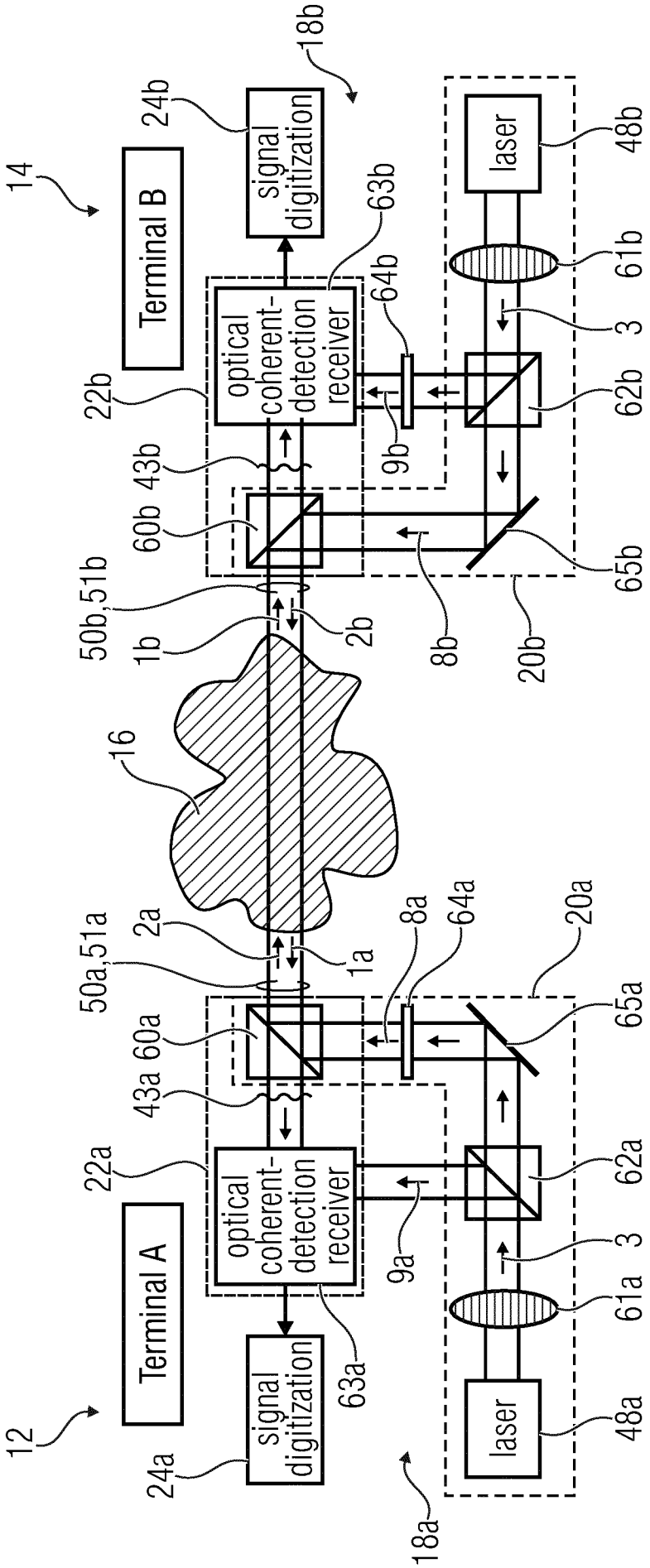
14
Terminal B
24b
signal digitization
18b
laser
48b
63b
61b
optical coherent-detection receiver
64b
3
22b
62b
9b
43b
60b
65b
50b,51b
1b
2b
8b
20b
16
2a
8a
64a
20a
50a,51a
1a
65a
43a
60a
22a
62a
optical coherent-detection receiver
9a
3
Terminal A
61a
63a
12
signal digitization
24a
laser
48a
18a

FIG 7

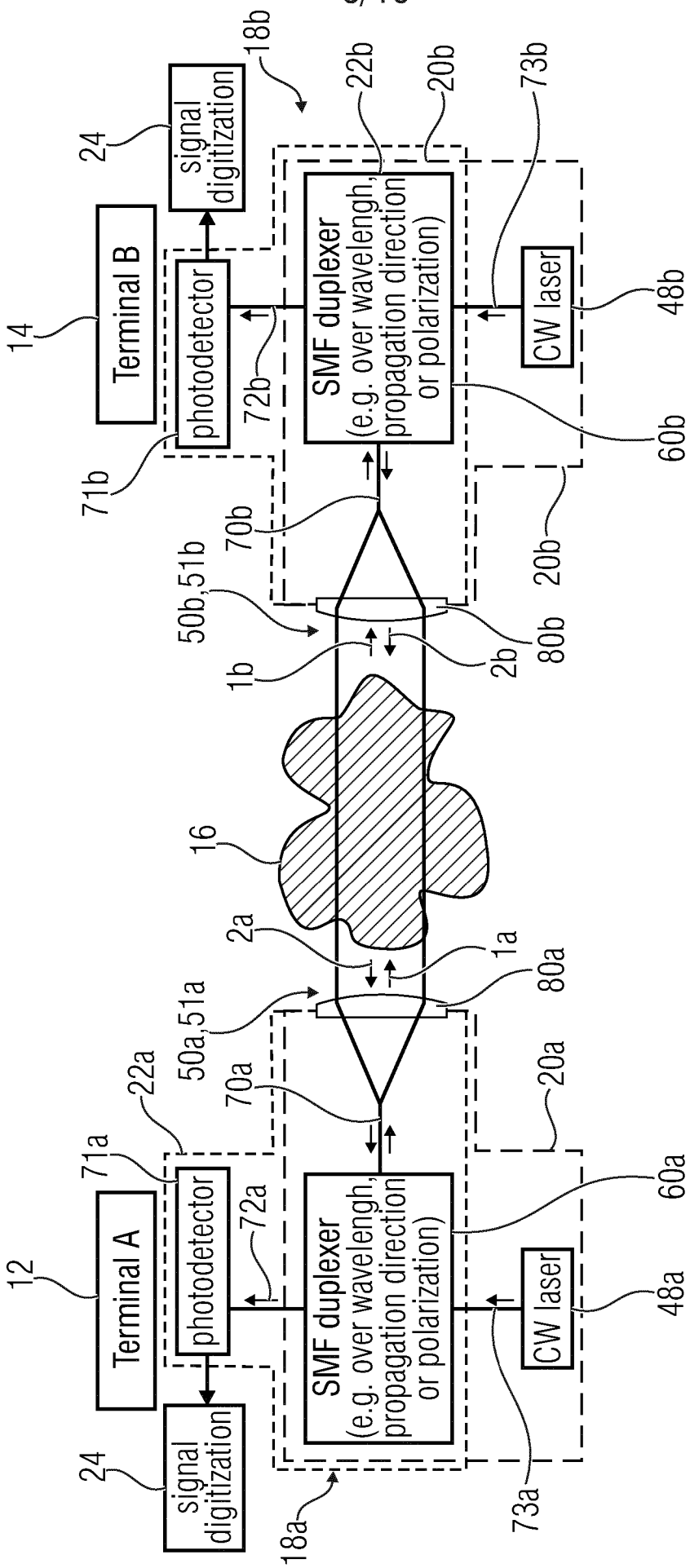
Terminal A
Terminal B
photodetector
signal digitization
SMF duplexer (e.g. over wavelengh, propagation direction or polarization)
CW laser
12
14
16
18a
18b
20a
20b
22a
22b
24
48a
48b
50a,51a
50b,51b
60a
60b
70a
70b
71a
71b
72a
72b
73a
73b
80a
80b
1a
1b
2a
2b

FIG 8

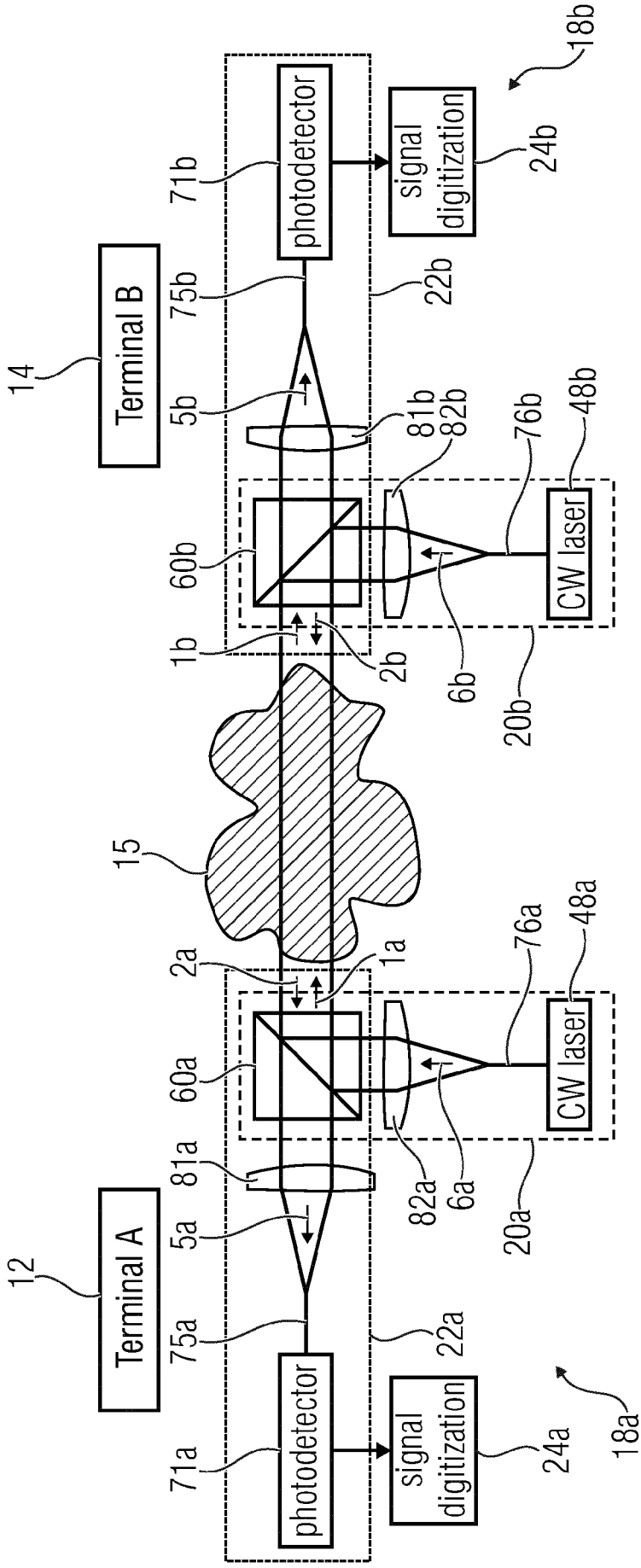
Terminal A
Terminal B
photodetector
signal digitization
CW laser
12
14
15
18a
18b
20a
20b
22a
22b
24a
24b
48a
48b
60a
60b
71a
71b
75a
75b
76a
76b
81a
81b
82a
82b
1a
1b
2a
2b
5a
5b
6a
6b

FIG 9

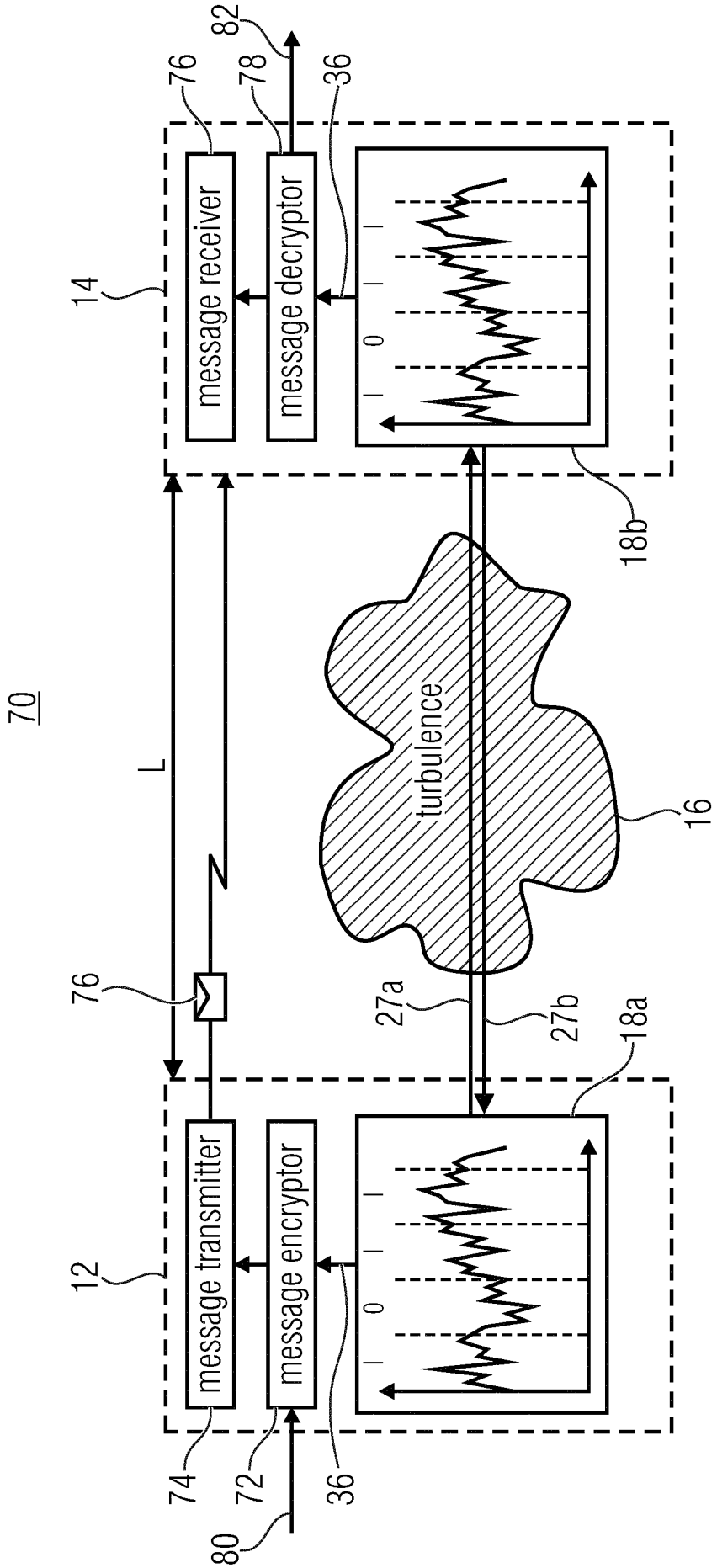
70
L
14
message receiver
message decryptor
76
78
36
82
18b
turbulence
16
27a
27b
18a
76
12
message transmitter
message encryptor
74
72
36
80

FIG 10

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/051855

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/12
ADD.

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)
H04L

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)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | DRAKE MARVIN D ET AL: "Optical key distribution system using atmospheric turbulence as the randomness generating function: classical optical protocol for information assurance", OPTICAL ENGINEERING, SOC. OF PHOTO-OPTICAL INSTRUMENTATION ENGINEERS, BELLINGHAM, vol. 52, no. 5, 1 May 2013 (2013-05-01), page 55008, XP060025827, ISSN: 0091-3286, DOI: 10.1117/1.OE.52.5.055008 [retrieved on 2013-05-29] cited in the application abstract; figures 3,4,5 Sections 5, 6 and 7 ----- -/-- | 1-15 |

[X] Further documents are listed in the continuation of Box C.

[X] 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 | Date of mailing of the international search report |
|---|---|
| 15 September 2015 | 29/09/2015 |

| Name and mailing address of the ISA/ | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040,<br>Fax: (+31-70) 340-3016 | Wolters, Robert |

1

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

# INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/051855

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2010/080386 A1 (DONNANGELO NICHOLAS C [US] ET AL) 1 April 2010 (2010-04-01) cited in the application abstract | 1-15 |
| A | YONGXIONG REN ET AL: "Heterodyne efficiency of a coherent free-space optical communication model through atmospheric turbulence", APPLIED OPTICS, OPTICAL SOCIETY OF AMERICA, WASHINGTON, DC; US, vol. 51, no. 30, 20 October 2012 (2012-10-20), pages 7246-7254, XP001578905, ISSN: 0003-6935, DOI: 10.1364/AO.51.007246 [retrieved on 2012-10-16] abstract; figure 1 Section 2 | 1-15 |
| A | TANG X ET AL: "Free-space optical communication employing polarization shift keying coherent modulation in atmospheric turbulence channel", COMMUNICATION SYSTEMS NETWORKS AND DIGITAL SIGNAL PROCESSING (CSNDSP), 2010 7TH INTERNATIONAL SYMPOSIUM ON, IEEE, PISCATAWAY, NJ, USA, 21 July 2010 (2010-07-21), pages 615-620, XP031759455, ISBN: 978-1-4244-8858-2 abstract; figure 2 | 1-15 |

1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2015/051855

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2010080386 A1 | 01-04-2010 | US 2010080386 A1 | 01-04-2010 |
| | | US 2012237031 A1 | 20-09-2012 |