(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 383 267 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 158(3) EPC

(43) Date of publication:
21.01.2004 Bulletin 2004/04

(21) Application number: **02713176.2**

(22) Date of filing: **20.03.2002**

(51) Int Cl.[7]: **H04L 9/38**, H04B 10/20

(86) International application number:
PCT/JP2002/002672

(87) International publication number:
WO 2002/076016 (26.09.2002 Gazette 2002/39)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **21.03.2001 JP 2001081501**

(71) Applicant: **JAPAN SCIENCE AND TECHNOLOGY CORPORATION**
Kawaguchi-shi, Saitama 332-0012 (JP)

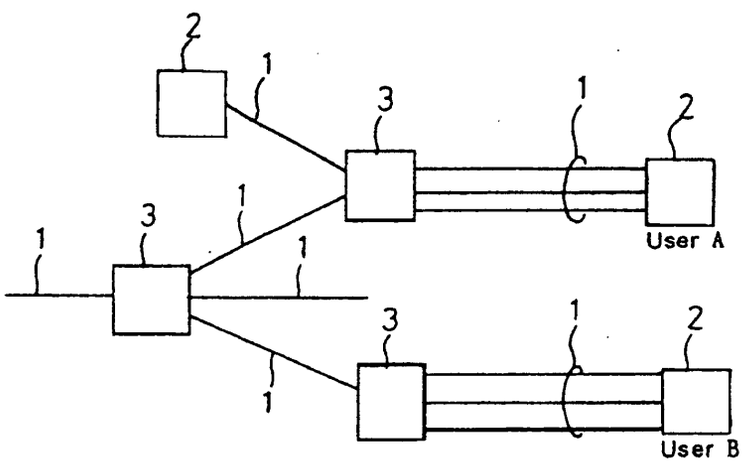
(72) Inventor: **TAKEUCHI, Shigeki**
Minami-ku,Sapporo-shi, Hokkaido 005-0004 (JP)

(74) Representative: **Jackson, Robert Patrick**
Frank B. Dehn & Co.,
European Patent Attorneys,
179 Queen Victoria Street
London EC4V 4EL (GB)

(54) QUANTUM CIPHER COMMUNICATION SYSTEM

(57) A quantum-cryptographic communication system for quantum-cryptographic communication in an optical network. The system comprises a transmitter for transmitting a packet signal having at least a light pulse train representing an address and a single photon pulse train used for quantum cryptography, and a router including a header analyzer for extracting the address information in the light pulse train from the packet signal and a gate switch for selecting one of optical fibers. The router routes the packet signal by selecting an optical fiber used for the next transmission path according to the extracted address information by the header analyzer and by switching the path to the selected optical fiber by the gate switch.

Fig. 1



EP 1 383 267 A1

Description

Technical Field

[0001] This invention relates to a quantum-cryptographic communication system, or in particular to a novel quantum-cryptographic communication system which can realize many-to-many key delivery in an optical network.

Background Art

[0002] In recent years, the quantum cryptography has been closely watched and vigorous research and development efforts have been made to realize the quantum cryptography as the next-generation cryptographic technology which may replace the common-key DES (Data Encryption Standard) cryptography and the public-key RSA (Rivest-Shamir-Adleman) cryptography. The information communication employing this quantum cryptography makes it possible for two parties located far from each other to share a secret key without the knowledge of third parties.

[0003] The quantum-cryptographic communication techniques which have so far been developed, however, are all based on the one-to-one or one-to-many key delivery using a specific fixed line. An attempt to conduct quantum-cryptographic communication in an optical network, therefore, requires the installation of an optical fiber dedicated to each user, thereby constituting an undesirable stumbling block to practical applications of the quantum-cryptographic communication on an optical network.

[0004] In order to solve this problem, a method of signal distribution through a beam splitter has been proposed (JP-A-9-502320). In this method, a multiplicity of keys are distributed from the transmitter at random to a multiplicity of users, and therefore the problem is posed that the rate at which the keys are delivered is reduced to 1/N with the increase in the number N of users.

[0005] The present invention has been achieved in view of this situation, and the object thereof is to obviate the problem of the prior art and provide a novel quantum-cryptographic communication system for realizing the many-to-many key delivery which allows a given user in an optical network to share a key with another specific user.

Disclosure of Invention

[0006] According to this invention, in order to solve the problem described above, there is provided a quantum-cryptographic communication system for conducting the quantum-cryptographic communication in an optical network configured of optical fibers, comprising a transmitter for transmitting a packet signal having at least a light pulse train representing an address and a single photon pulse train used for quantum cryptography, and a plurality of routers each including a header analyzer for extracting the address information in the light pulse train from the packet signal and a gate switch for switching to each optical fiber, characterized in that each router routes the packet signal by selecting an optical fiber constituting the next transmission path based on the address information detected by the header analyzer and switching the path to the selected optical fiber by the gate switch.

Brief Description of Drawings

[0007]

Fig. 1 is a diagram illustrating a general configuration of a quantum-cryptographic communication system according to this invention.
Fig. 2 is a graph illustrating a pulse signal in an quantum-cryptographic communication system according to this invention.
Fig. 3 is a diagram illustrating an internal configuration of a router in a quantum-cryptographic communication system according to this invention.

[0008] In the drawings, the reference numerals designate the following component parts:

1	Optical fiber
2	Transmitter
3	Router
31	Header analyzer
32	Gate switch

Best Mode for Carrying Out the Invention

[0009] This invention has the above-mentioned feature, and an embodiment thereof will be explained below.

[0010] Figs. 1 to 3 are diagrams for explaining a quantum-cryptographic communication system according to this invention. Fig. 1 illustrates a general configuration of a quantum-cryptographic communication system according to this invention comprising a transmitter (2) and routers (3) on an optical network configured of optical fibers (1), Fig. 2 illustrates a pulse signal, and Fig. 3 illustrates an internal configuration of the router (3).

[0011] As illustrated in Figs. 1 to 3, for example, this invention comprises a transmitter (2) for transmitting a packet signal having at least a light pulse train representing an address and a single photon pulse train used for the quantum cryptography, and routers (3) each including a header analyzer (31) for detecting the address information of the light pulse train from the packet signal sent by the transmitter (2) and a gate switch (32) for switching to each optical fiber (1).

[0012] Each router (3) selects an optical fiber (1) making up the next transmission path based on the address information detected by the header analyzer (31) and

switches to the particular optical fiber (1) by the gate switch (32), thereby routing the packet signal. As a result, the packet signal containing a single photon pulse train is transmitted progressively to an appropriate optical fiber (1) each time it passes through a router (3).

[0013] Specifically, the quantum-cryptographic communication system according to this invention can transmit a single photon train used for the quantum cryptography to a multiplicity of users including a given user A and a specific user B in the optical network by routing through the packet communication technique. Thus, the communication using the quantum cryptography becomes possible from each home equipped with optical fibers to a base station, for example, and the quantum cryptography can be used for domestic applications, thereby realizing the many-to-many quantum-cryptographic communication.

[0014] The transmitter (2) includes, though not shown, a quantum cryptography means, a packet signal production means and a packet signal transmitting means. The single photon pulse train of the quantum cryptography produced by the quantum cryptography means is split into packet signals by the packet signal production means. After adding a light pulse train constituting a header representing the address for each packet signal, the particular packet signal is sent by the packet signal transmitting means to an optical fiber (1) connected. A plurality of routers (3) are arranged on the optical network configured of the optical fibers (1), so that the packet signals are routed between the routers (3).

[0015] In the packet signal illustrated in Fig. 2, the light pulse train and the single photon pulse train are temporally divided. As long as the address information can be detected by the header analyzer (31) of the router (3), however, the light pulse train and the single photon pulse train may be mixed or divided into different frequencies. The address information can be detected by the header analyzer (31) through any of well-known various methods used for the packet communication.

[0016] The light pulse train can contain not only the header representing an address (such as the destination IP address) but also a signal pulse used for the normal traditional communication.

[0017] Further, the router (3) may be configured only of optical switches. In such a case, the gate switch (32) is kept open for a predetermined time length by the optical nonlinearity of the light pulse train (header portion), and while the gate switch (32) is open, the packet signal containing the single photon pulse train is transmitted to the next optical fiber (1).

[0018] This invention is not of course limited to the above-mentioned examples, but the details thereof may be variously modified.

Industrial Applicability

[0019] As explained in detail above, according to this invention, there is provided a novel quantum-cryptographic communication system in which a key can be shared by a given user and another specific user in an optical network, thereby making it possible to realize the many-to-many quantum-cryptographic communication.

Claims

1. A quantum-cryptographic communication system for conducting quantum-cryptographic communication in an optical network configured of optical fibers, comprising:

a transmitter for transmitting a packet signal having at least a light pulse train representing an address and a single photon pulse train used for the quantum cryptography; and
a plurality of routers each including a header analyzer for detecting the address information of the light pulse train from the packet signal and a gate switch for switching to each optical fiber;

characterized in that each of the routers selects an optical fiber constituting the next transmission path based on the address information detected the header analyzer, and switches to the particular optical fiber through the gate switch, thereby routing the packet signal.

Fig. 1

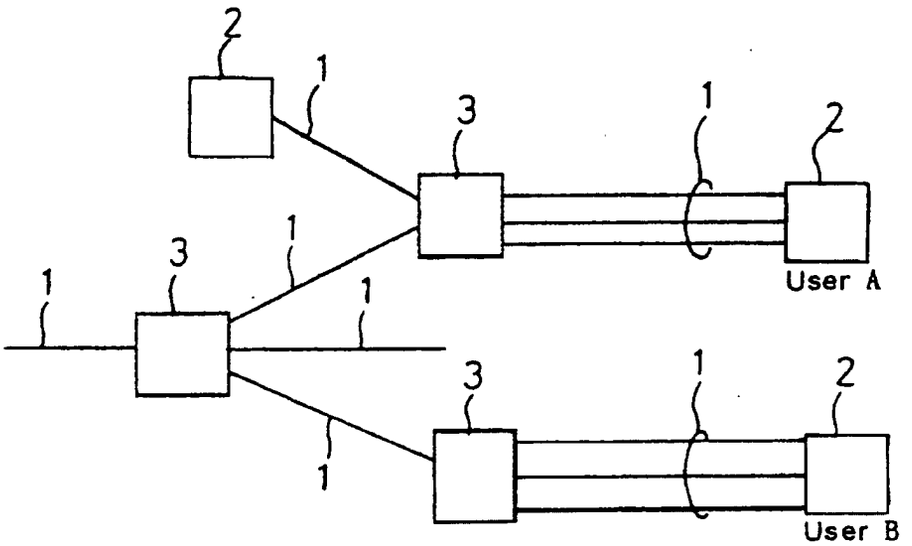


Fig. 2

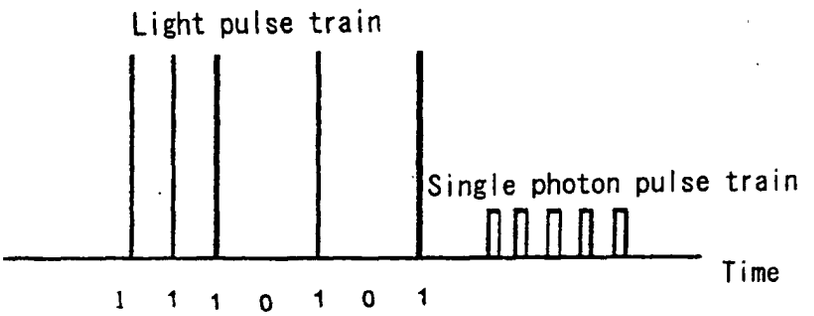
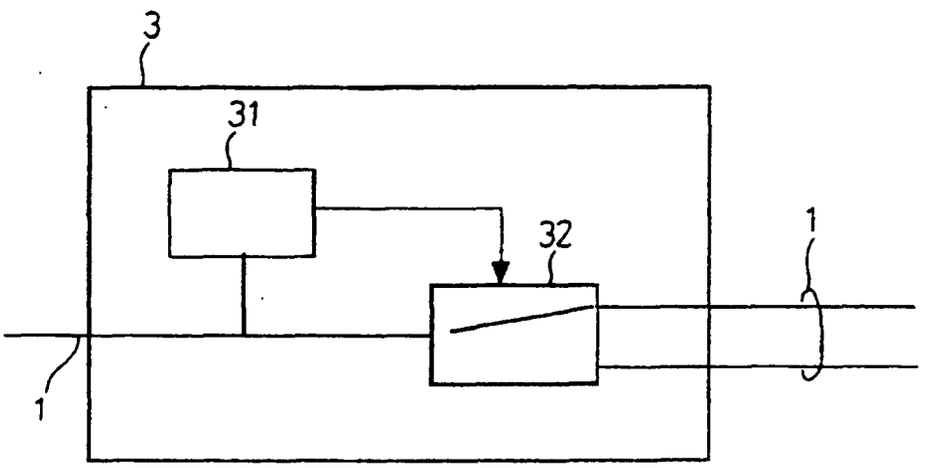


Fig. 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/02672

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/38, H04B10/20

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)
Int.Cl[7] H04L9/38, H04B10/20

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

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 6-261073 A (Nippon Telegraph And Telephone Corp.), 16 September, 1994 (16.09.94), Full text; Figs. 1 to 5 (Family: none)	1

☐ 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 document 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
01 May, 2002 (01.05.02)	21 May, 2002 (21.05.02)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)