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

(11) EP 1 383 267 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
24.05.2006 Bulletin 2006/21

(21) Application number: **02713176.2**

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

(51) Int Cl.:
H04L 9/08 *(2006.01)*

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

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

(54) **QUANTUM CIPHER COMMUNICATION SYSTEM**

KOMMUNIKATIONSSYSTEM MIT QUANTENCHIFFRIERUNG

SYSTEME DE COMMUNICATION CRYPTOGRAPHIQUE QUANTIQUE

(84) Designated Contracting States:
CH DE FR GB LI

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

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

(73) Proprietor: **Japan Science and Technology Agency**
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.
St Bride's House
10 Salisbury Square
London EC4Y 8JD (GB)

(56) References cited:
JP-A- 6 261 073 **US-A- 5 768 378**

EP 1 383 267 B1

Printed by Jouve, 75001 PARIS (FR)

Description

[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.

[0002] In recent years, quantum cryptography has been closely watched and vigorous research and development efforts have been made to realize 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.

[0006] JP-A-9-502320 discloses a quantum-cryptographic communication system for conducting quantum-cryptographic communication in an optical network configured of optical fibers, comprising a transmitter for transmitting a signal including a single photon pulse train used for the quantum-cryptography.

[0007] The present invention is characterised in that a transmitter produces 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 transmits the produced packet signal to an optical fiber connected thereto, the system further comprising a plurality of routers each including a header analyzer for detecting the address information in the light pulse train from the packet signal and an optical gate switch for switching to each optical fiber, and each of the routers selects an optical fiber constituting the next transmission path based on the address information detected by the header analyzer and switches the path to the selected optical fiber through the optical gate switch, thereby routing the packet signal.

[0008] The present invention also provides a method of conducting quantum cryptographic communication in an optical network configured of optical fibres, comprising: transmitting a packet signal including a light pulse train representing an address and a single photon pulse train used for the quantum cryptography; and routing the packet signal by detecting the address information of the light pulse train using a header analyser, selecting an optical fibre constituting the next transmission path based on the address information, and switching the packet to the correct optical fibre using an optical gate switch.

[0009] An embodiment of the present invention will now be described by way of example only and with reference to the accompanying drawings, in which:

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.

[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.

[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 (1), comprising:

   a transmitter (2) for transmitting a signal including a single photon pulse train used for the quantum cryptography; **characterised in that** the transmitter is adapted to produce 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 to transmit the produced packet signal to an optical fiber connected thereto; said system further comprising

   a plurality of routers (3) each including a header analyzer (31) for detecting the address information of the light pulse train from the packet signal and an optical gate switch (32) for switching to each optical fiber; and

   each of the routers being adapted to select an optical fiber constituting the next transmission path based on the address information detected by the header analyzer, and to switch to the particular optical fiber through the optical gate switch, thereby routing the packet signal.

2. A method of conducting quantum cryptographic communication in an optical network configured of optical fibres (1), **characterized by**:

   transmitting a packet signal including a light pulse train representing an address and a single photon pulse train used for the quantum cryptography; and

   routing the packet signal by detecting the address information of the light pulse train using a header analyser (31), selecting an optical fibre constituting the next transmission path based on the address information, and switching the packet to the correct optical fibre using an optical gate switch.

Patentansprüche

1. Ein Quantenkryptografiekommunikationssystem zum Durchführen einer Quantenkryptografiekommunikation in einem optischen Netzwerk, das aus Glasfasern (1) aufgebaut ist, umfassend:

   einen Sender (2) zum Senden eines Signals, welches eine einzelne Photonenimpulsfolge enthält, die für die Quantenkryptografie verwendet wird; **dadurch gekennzeichnet, dass** der Sender eingerichtet ist, um ein Paketsignal mit mindestens einer Lichtimpulsfolge zu erzeugen, welche eine Adresse und eine einzelne Photonenimpulsfolge repräsentiert, die für die Quantenkryptografie verwendet wird, und um das erzeugte Paketsignal an eine Glasfaser zu übertragen, die damit verbunden ist; wobei das System des Weiteren umfasst:

eine Mehrzahl von Routern (3), wobei jeder einen Headeranalysator (31) zum Detektieren der Adressinformation der Lichtimpulsfolge aus dem Paketsignal und eine optische Gatterschaltung (22) zum Umschalten auf jede Glasfaser umfasst; und
wobei jeder der Router eingerichtet ist, um eine Glasfaser, welche den nächsten Übertragungsweg bildet, basierend auf der Adressinformation auszuwählen, die durch den Headeranalysator detektiert wird, und um durch die optische Gatterschaltung auf die bestimmte Glasfaser umzuschalten, wodurch das Paketsignal weitergeleitet wird.

2. Ein Verfahren zum Durchführen einer Quantenkryptografiekommunikation in einem optischen Netzwerk, das aus Glasfasern (1) aufgebaut ist, **gekennzeichnet durch**:

Übertragen eines Paketsignals, umfassend eine Lichtimpulsfolge, welche eine Adresse und eine einzelne Photonenimpulsfolge repräsentiert, die für die Quantenkryptografie verwendet wird; und
Weiterleiten des Paketsignals **durch** Detektieren der Adressinformation der Lichtimpulsfolge, wobei ein Headeranalysator (31) verwendet wird, Auswählen einer Glasfaser, welche den nächsten Übertragungsweg bildet, basierend auf der Adressinformation, und Umschalten des Pakets auf die richtige Glasfaser, wobei eine optische Gatterschaltung verwendet wird.

Revendications

1. Système de communication cryptographique quantique destiné à conduire une communication cryptographique quantique dans un réseau optique configuré avec des fibres optiques (1), comprenant :

un émetteur (2) destiné à transmettre un signal comprenant un train d'impulsion photonique unique utilisé pour la cryptographie quantique ; **caractérisé en ce que** l'émetteur est adapté pour produire un signal de paquet ayant au moins un train d'impulsion lumineuse représentant une adresse et un train d'impulsion photonique unique utilisé pour la cryptographie quantique, et pour transmettre le signal de paquet produit vers une fibre optique connectée à celui-ci ; ledit système comprenant en outre
une pluralité de routeurs (3) comprenant chacun un analyseur d'en-tête (31) destiné à détecter l'information d'adresse du train d'impulsion lumineuse à partir du signal de paquet, et un commutateur de porte optique (32) destiné à la commutation vers chaque fibre optique ; et
chacun des routeurs étant adapté pour sélectionner une fibre optique constituant la voie de transmission suivante sur la base de l'information d'adresse détectée par l'analyseur d'en-tête, et pour commuter vers la fibre optique particulière par le biais du commutateur de porte optique, routant de ce fait le signal de paquet.

2. Procédé de conduite d'une communication cryptographique quantique dans un réseau optique configuré avec des fibres optiques (1), **caractérisé par** :

la transmission d'un signal de paquet comprenant un train d'impulsion lumineuse représentant une adresse et un train d'impulsion photonique unique utilisé pour la cryptographie quantique ; et
le routage du signal de paquet en détectant l'information d'adresse du train d'impulsion lumineuse au moyen d'un analyseur d'en-tête (31), la sélection d'une fibre optique constituant la voie de transmission suivante sur la base de l'information d'adresse, et la commutation du paquet vers la fibre optique correcte en utilisant un commutateur de porte optique.

Fig. 1

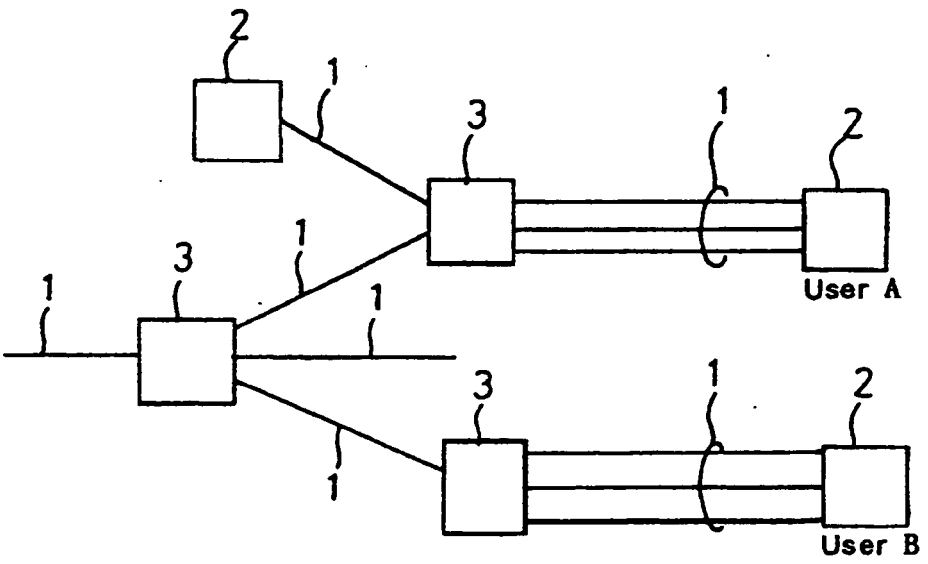

Fig. 2

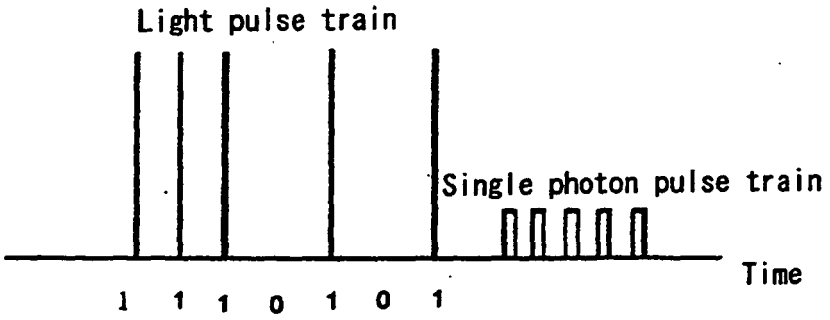

Fig. 3