

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
1 November 2007 (01.11.2007)

PCT

(10) International Publication Number  
**WO 2007/123869 A2**

(51) International Patent Classification:  
*H04K 1/04* (2006.01)

(21) International Application Number:  
PCT/US2007/009236

(22) International Filing Date: 16 April 2007 (16.04.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
60/792,764 18 April 2006 (18.04.2006) US

(71) Applicant (for all designated States except US): **MAGIQ TECHNOLOGIES, INC.** [US/US]; 171 Madison Avenue, Suite 1300, New York, NY 10016 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **GELFOND, Robert** [US/US]; 45 E. 25th St., #39B, New York, NY 10010 (US). **BERZANSKIS, Audrius** [LT/US]; 764 Cambridge St., #8, Cambridge, MA 02141 (US).

(74) Agent: **GORTYCH, Joseph, E.**; Opticus IP Law PLLC, 7791 Alister Mackenzie DR, Sarasota, FL 34240 (US).

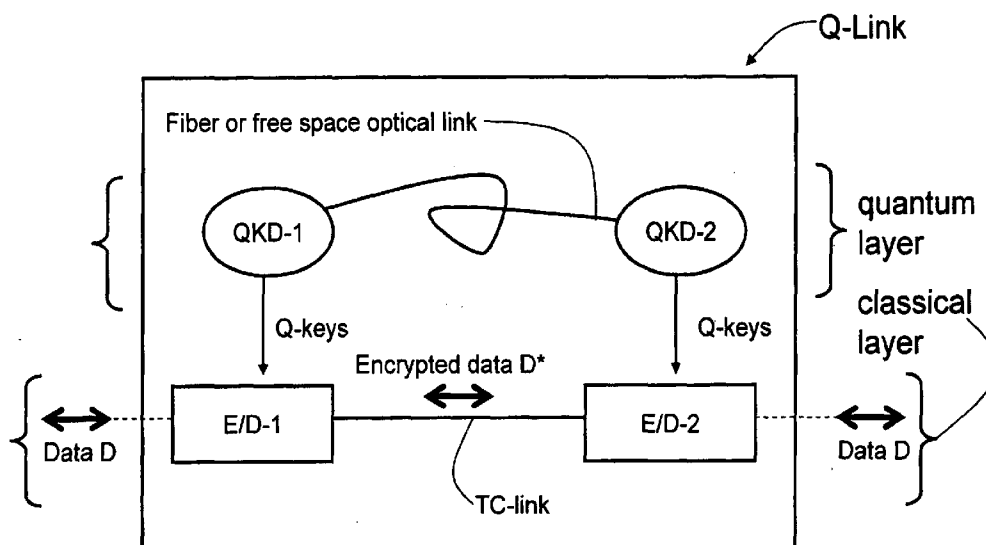
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:  
— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: KEY MANAGEMENT AND USER AUTHENTICATION FOR QUANTUM CRYPTOGRAPHY NETWORKS



(57) Abstract: Key management and user authentication systems and methods for quantum cryptography networks that allow for users securely communicate over a traditional communication link (TC-link). The method includes securely linking a centralized quantum key certificate authority (QKCA) to each network user via respective secure quantum links or "Q-links" that encrypt and decrypt data based on quantum keys ("Q-keys"). When two users (Alice and Bob) wish to communicate, the QKCA sends a set of true random bits (R) to each user over the respective Q-links. They then use R as a key to encode and decode data they send to each other over the TC-link.

WO 2007/123869 A2

## **KEY MANAGEMENT AND USER AUTHENTICATION FOR QUANTUM CRYPTOGRAPHY NETWORKS**

### **Claim of Priority**

This application claims the benefit of priority of U.S. Provisional Patent Application Serial No. 60/792,764, filed on April 18, 2006.

### **Technical Field of the Invention**

The present invention relates to quantum communication, and in particular relates to and has industrial utility in connection with systems and methods of key management and user authentication in quantum cryptography networks.

### **Background Art**

QKD involves establishing a key between a sender ("Alice") and a receiver ("Bob") by using either single-photons or weak (e.g., 0.1 photon on average) optical signals (pulses) called "qubits" or "quantum signals" transmitted over a "quantum channel." Unlike classical cryptography whose security depends on computational impracticality, the security of quantum cryptography is based on the quantum mechanical principle that any measurement of a quantum system in an unknown state will modify its state. As a consequence, an eavesdropper ("Eve") that attempts to intercept or otherwise measure the exchanged qubits will introduce errors that reveal her presence.

The general principles of quantum cryptography were first set forth by Bennett and Brassard in their article "Quantum Cryptography: Public key distribution and coin tossing," Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179 (IEEE, New York, 1984). Specific QKD systems are described in U.S. Patent No. 5,307,4100 to Bennett, and in the article by C.H. Bennett entitled "Quantum Cryptography Using Any Two Non-Orthogonal States", Phys. Rev. Lett. 68 3121 (1992). The general process for performing QKD is described in

the book by Bouwmeester et al., "The Physics of Quantum Information," Springer-Verlag 20001, in Section 2.3, pages 27-33.

QKD systems were first developed in the form of a simple point-to-point connection between two users, called "Alice" and "Bob." Nowadays, QKD systems are being considered as part of QKD-based networks that include multiple users as nodes in a dedicated QKD-system network, or multiple users incorporated into an existing classical telecommunications network.

The extension of QKD from point-to-point communication to network-type communication introduces some logistical issues. For example, QKD-based networks require the multiple users to have a process for establishing a common "quantum key" between any two users prior to their communicating with each other, even if they have never communicated with each other and/or even if they do not have a direct communication link. Furthermore, in view of the fact that a given user will often need to selectively communicate with one or just a few of the total number of users, there needs to be a way to authenticate the users with whom they are communicating to ensure their message is shared with a party intended to receive the message. In addition, quantum cryptography employs symmetric keys rather than public keys used with public key infrastructure (PKI) cryptography.

### **Description of the Invention**

An aspect of the invention is a method of establishing a secure communication link between first and second users Alice and Bob connected by a traditional communication link. The method includes establishing first and second secure quantum links (Q-links) between a quantum key certification authority (QKCA) and Alice and Bob, respectively. The method also includes generating at the QKCA a set R of truly random bits, and distributing R over the respective Q-links to Alice and Bob. The method also includes Alice and Bob using R as an encryption key to securely communicate over the traditional communication link.

**Brief Description of the Drawing**

FIG. 1 is a schematic diagram of a Q-link as used in the present invention;

FIG. 2 is a schematic diagram of a first example of a star-topology Q-network that includes the QKI architecture of the present invention;

FIG. 3 is a detailed schematic diagram of an example quantum key certificate authority (QKCA) module that serves as a key manager and authentication center for the QKI architecture;

FIG. 4 is a schematic diagram of a first example of a star-topology Q-network that includes the QKI architecture of the present invention similar to that of FIG. 2, but that includes two QKCA modules Q-linked to one another; and

FIG. 5 is a schematic diagram of a portion of the Q-network of FIG. 2, illustrating how the QKI architecture of the present invention is used to authenticate a new Q-link established between Alice and Bob.

The various elements depicted in the drawing are merely representational and are not necessarily drawn to scale. Certain sections thereof may be exaggerated, while others may be minimized. The drawing is intended to illustrate an example embodiment of the invention that can be understood and appropriately carried out by those of ordinary skill in the art.

**Detailed Description of the Invention**

FIG. 1 is a schematic diagram of a quantum link or "Q-link" in which a communication channel is protected by quantum cryptography (e.g., quantum key distribution or "QKD"). In its basic form, the Q-link includes a quantum layer having two operably coupled QKD stations, QKD-1 and QKD-2, and a classical layer having a classical (traditional) communication line protected by a

symmetric key encryption protocol (e.g., one-time pad) that employs quantum keys provided by the QKD stations.

The classical layer includes encryptor/decryptor (E/D) units ED-1 and ED-2 coupled to respective QKD stations QKD-1 and QKD-2. The E/D units are adapted to receive data  $D$ , encrypt the data to form encrypted data  $D^*$  and then transmit the encrypted data  $D^*$  over the traditional communication channel. Likewise, each E/D unit is adapted to receive encrypted data  $D^*$  and decrypt it to recover data  $D$ . The encrypting and decrypting of data is performed using  $Q$ -keys provided by the quantum layer.

### **Example embodiments**

The present invention refers to a "quantum network" or "Q-network," which describes a communication infrastructure that includes  $Q$ -links and a traditional network communication infrastructure with a number  $n$  of users. The present invention employs a novel key management and authentication architecture. Example embodiments of how the QKI architecture of the present invention is used in  $Q$ -networks are described below.

#### ***First example embodiment***

FIG. 2 illustrates an example of a star-topology  $Q$ -network 100 that includes an example embodiment of the QKI architecture according to the present invention. The QKI architecture in  $Q$ -network 100 includes a Quantum Key Certificate Authority, or QKCA.

FIG. 3 is a schematic diagram of an example embodiment of a QKCA according to the present invention. The QKCA is a trusted third party, i.e., it is an entity that issues authentication certificates (ACs) for use by other parties. Its functionality is similar to that of Certificate Authority in PKI. It is a point where  $Q$ -links are securely terminated. A  $Q$ -link provides an authenticated link between an end user and QKCA. On the other hand, two  $Q$ -links connected via a trusted third party—here, the QKCA—provide an authenticated channel for the end points (users).

Though in general the functionality of QKCA is similar to that of CA in PKI, there are some differences. A public key CA issues digital certificates that couple the identity of a network user to its public key. In quantum cryptography, there is no such public key. Rather, the keys are symmetric. The QKCA extends the conventional CA by adding Q-key management functionality. In parallel to the "quantum" functionality, the QKCA can still operate as a standard CA providing standard PKI functions to the users connected to QKCA via traditional communication links ("TC-links"). From this point of view, QKCA provides a superset of cryptographic operations in comparison to CA.

The very presence of a Q-link between QKCA and a user U ensures a channel of authenticated communication between the two. Initial authentication occurs during the installation of the Q-link. The authentication keys can be refreshed by quantum keys generated by QKD in Q-link and this has to be defined by the security policies of the network.

With continuing reference to FIG. 3, the QKCA has a policy manager and a User Rights Database that includes information on the users U of the Q-network, along with their respective rights and security definitions. All requests from the users U come to a Policy Manager, which consults the User Rights Database and makes a decision whether to deny or to allow the requested operation. In an example embodiment, the User Rights Database contains information about the communication security requirements among users.

For example, user  $U_3$  who only has a TC-link TCL-3 with the QKCA may ask to establish a communication session with a user  $U_1$  connected via a Q-link QL-1 with the QKCA. The Policy Manager consults the User Rights Database to see if user  $U_1$  is allowing communication with user  $U_3$  over links protected just by traditional cryptography. If not, the Policy Manager denies that request. Otherwise, the Policy Manager allows a communication session to be established.

The QKCA also includes a Session Manager that gets involved in case the communication request is approved by the policy manager. The Session Manager creates a communication session between two users. In case the users  $U$  are connected by Q-links with the QKCA, the Session Manager provides them with sets of random bits  $R$  from a TRNG Unit. The random bits  $R$  are used for encrypting direct communication between the users. The TRNG Unit can be any one of the known types of truly random number generators. Note that the communication between such users is protected by the highest level of security provided by quantum cryptography even though the users are not connected by a QKD device of any sort; they also need not share any optical communication line.

If the users  $U$  are connected with the QKCA by TC-links, then the functionality of the QKCA replicates that of conventional CA in PKI.

The QKCA also includes interfaces to the different communication channels, namely the Q-links and the TC-links.

There is more variety when one of the users is connected with the QKCA via a TC-link and the other via a Q-link. Depending on the policies set by the users, the whole scheme might switch to the standard PKI communication scheme as in the case of two TC-links, or they might decide to keep the strongest possible level of cryptography on the Q-link while doing traditional PKI based communication on the TC-link. In the latter case, the session manager provides set of random bits  $R$  to one user over the Q-link, and the same set to the other user over the TC-link encrypted by traditional cryptography.

The highest level of security is achieved only when the communicating parties share Q-links with the QKCA.

With reference again to FIG. 2, users  $U$  in Q-network 100 can only establish secure keys through the QKCA. For  $n$  network users  $U$ , if a subset of  $i$  users ( $i < n$ ) want to communicate secrets amongst each other, then each of

the  $i$  users contacts the QKCA with a request to establish a communication session.

With continuing reference to FIG. 2, Q-network 100 includes a number  $n$  of network users  $U$  ( $U_1, U_2, \dots U_n$ ) operably linked to the QKCA via Q-links  $QL$  ( $QL-1, QL-2, \dots QL-n$ , respectively). The  $n$  users include two users Alice and Bob operatively coupled to the QKCA via respective Q-links  $QL-A$  and  $QL-B$ . The  $n$  users  $U$  are also linked by TC-links  $TCL$ , with one such link being  $TCL-AB$  between Alice and Bob.

The two main initial conditions of Q-network 100 are that all  $n$  users  $U$  trust the QKCA, and that Alice wants to communicate with Bob, though they are not directly connected by a Q-link. The only direct link between Alice and Bob is the TC-link  $CL-AB$ . The protocol Alice and Bob follow in order to securely communicate is as follows. First, Alice issues a communication request to the QKCA over Q-link  $QL-A$  stating that she wishes to communicate with Bob. The QKCA passes the communication request to Bob via Q-link  $QL-B$ . If Bob responds to the QKCA that he wishes to communicate with Alice, then the QKCA sends a stream (set)  $R$  of truly random bits to Alice over Q-link  $QL-A$  and to Bob over Q-link  $QL-B$ . Recall, when set  $R$  is sent over a Q-link, it is encrypted and decrypted with a Q-key associated with the Q-link (see FIG. 1). Set  $R$  is generated by the TRNG Unit. Set  $R$  can be any random number unknown to all the users  $U$  except the users requesting communication.

At this point, Alice and Bob now share set  $R$  as generated by the QKCA. Alice and Bob then use set  $R$  as a key for securely communicating over any classical communication channel, such as the TC-link  $CL-AB$ .

### ***Second example embodiment***

FIG. 4 is a schematic diagram of a second example embodiment of a star-topology Q-network 200 that employs another example embodiment of the QKI architecture of the present invention. Q-network 200 is similar to that of FIG. 2, but includes two QKCAs, labeled QKCA-A and QKCA-B, operably

coupled to one another by a Q-link QL-AB. Q-network 200 has  $n$  network users UA (UA1, UA2, ... UA $n$ ) operably linked to the QKCA-A via respective Q-links QLA-1, QLA-2, ... QLA- $n$ . One of the  $n$  users is user Alice.

Likewise, Q-network 200 has  $m$  additional network users UB (UB1, UB2, ... UB $m$ ) operably linked to the QKCA-B via Q-links QLB-1, QLB-2, ... QLB- $m$ , respectively, including user Bob. The  $n$  users UA are also linked directly to each other and to the  $m$  users UB only via TC-links TCL, of which one such link TCL-AB is shown between Alice and Bob.

The two main initial conditions of Q-network 200 are that all  $n$  users UA and  $m$  users UB trust the QKCA-A and the QKCA-B, and that Alice wants to securely communicate with Bob, though they are only directly connected by TC-link TCL-AB.

The protocol Alice and Bob follow to securely communicate with one another over their TC-link TCL-AB is as follows. First, Alice issues a communication request to the QKCA-A over Q-link QL-A that she wishes to communicate with Bob. The QKCA-A routes this communication request to the QKCA-B over Q-link QL-AB, and the QKCA-B routes the communication to Bob over Q-Link QLB-B. If Bob accepts the communication request, then the QKCA-B generates a set R of truly random bits and sends R to both Bob and the QKCA-A over the corresponding Q-Links. The QKCA-A routes R to Alice over Q-link QL-A. Note that either the QKCA-A or the QKCA-B can generate R; The QKCA-B was chosen in the present example for the sake of illustration.

#### ***Other aspects of the QKI architecture***

The QKI session can function in a streaming mode wherein Q-keys are streamed to users continuously or in a key-per-request mode wherein Q-keys of a given length are provided to each user per request.

***New Q-link user authentication***

The QKI Q-network architecture of the present invention can be used to authenticate two users. FIG. 4 is the Q-network 100 of FIG. 1, showing just the two users Alice and Bob linked to the QKCA via Q-links QL-A and QL-B. In the present example embodiment, Alice and Bob are to be linked directly by a new Q-link QL-AB' (dashed line). Authentication is required to start QKD over the new Q-link.

The authentication protocol in this case involves either Alice or Bob requesting the QKCA to allow communication with the other over the direct Q-link QL-AB'. In response to an affirmative request by the other party, the QKCA provides Alice and Bob with an AC that includes a set R of truly random bits. Alice and Bob then use set R as an authentication key to set up a QKD session using their direct Q-link QL-AB'.

What is claimed is:

1. A method of establishing a secure communication link between first and second users Alice and Bob connected by a traditional communication link (TC-link), comprising:

establishing first and second secure quantum links (Q-links) between a quantum key certification authority (QKCA) and Alice and Bob, respectively;

at the QKCA, generating a set R of truly random bits, and distributing set R over the respective Q-links to Alice and Bob; and

Alice and Bob using set R as an encryption key to securely communicate over a the TC-link.

2. The method of claim 1, including:

at Alice, encrypting data D using set R as an encryption key to form encrypted data D\* and transmitting D\* over the TC-link directly to Bob; and

at Bob, receiving and decrypting D\* using set R as a decryption key to recover data D.

3. A method of authenticating first and second users in a quantum network (Q-network) coupled by a new Q-link QL-AB', comprising:

the first user requesting a quantum key certificate authority (QKCA) to allow communication with the second user over the direct Q-link QL-AB';

the QKCA providing the first and second users with a set R of truly random bits over respective first and second Q-links connecting the first and second users to the QKCA; and

the first and second users using set R as a key to initially communicate over new Q-link QL-AB' and authenticate the other party.

4. The method of claim 3, wherein once the first and second users are authenticated, each obtaining quantum keys (Q-keys) from the QKCA.

5. The method of claim 3, wherein once the first and second users are authenticated, establishing quantum keys (Q-keys) between the first and second users over the direct Q-link QL-AB.

6. A method of establishing a secure communication link between first and second users Alice and Bob in a quantum network ("Q-network") where Alice and Bob are in direct communication only via a traditional communication link (TC-link) and in direct communication with respective first and second quantum key certification authorities (QKCA) via respective first and second Q-links, comprising:

    sending a set R of truly random bits from the second QKCA to Bob over the first Q-link;

    sending the set R from the second QKCA to the first QKCA over a third Q-link connecting the first and second QKCA;

    sending the set R from the first QKCA to Alice over the second Q-link;

and

    Alice and Bob using R as a key to encrypt and send information over the TC-link.

7. A key management system for a quantum network (Q-network) comprising:

    a centralized quantum key certificate authority (QKCA) having a number of users U directly linked thereto via respective quantum links (Q-links) and directly linked to each other via traditional communication links;

    wherein the QKCA unit includes a session manager and a true random number generator that operate to provide a set R of truly random bits to two or more of the users U via respective two or more Q-links; and

    wherein each of the two or more users U is adapted to use set R as a key for securely communicating and authenticating with other users.

8. A method of establishing a secure communication link between first and second users Alice and Bob connected by a first traditional communication link (TC-link), comprising:

establishing a secure quantum link (Q-link) between a quantum key certification authority (QKCA) and Alice;

establishing a second TC-link between the QKCA and Bob;

at the QKCA, generating a set R of truly random bits, and distributing set R to Alice over the Q-link and to Bob over the second TC-link; and

Alice and Bob using set R as an encryption key to securely communicate over the first TC-link.

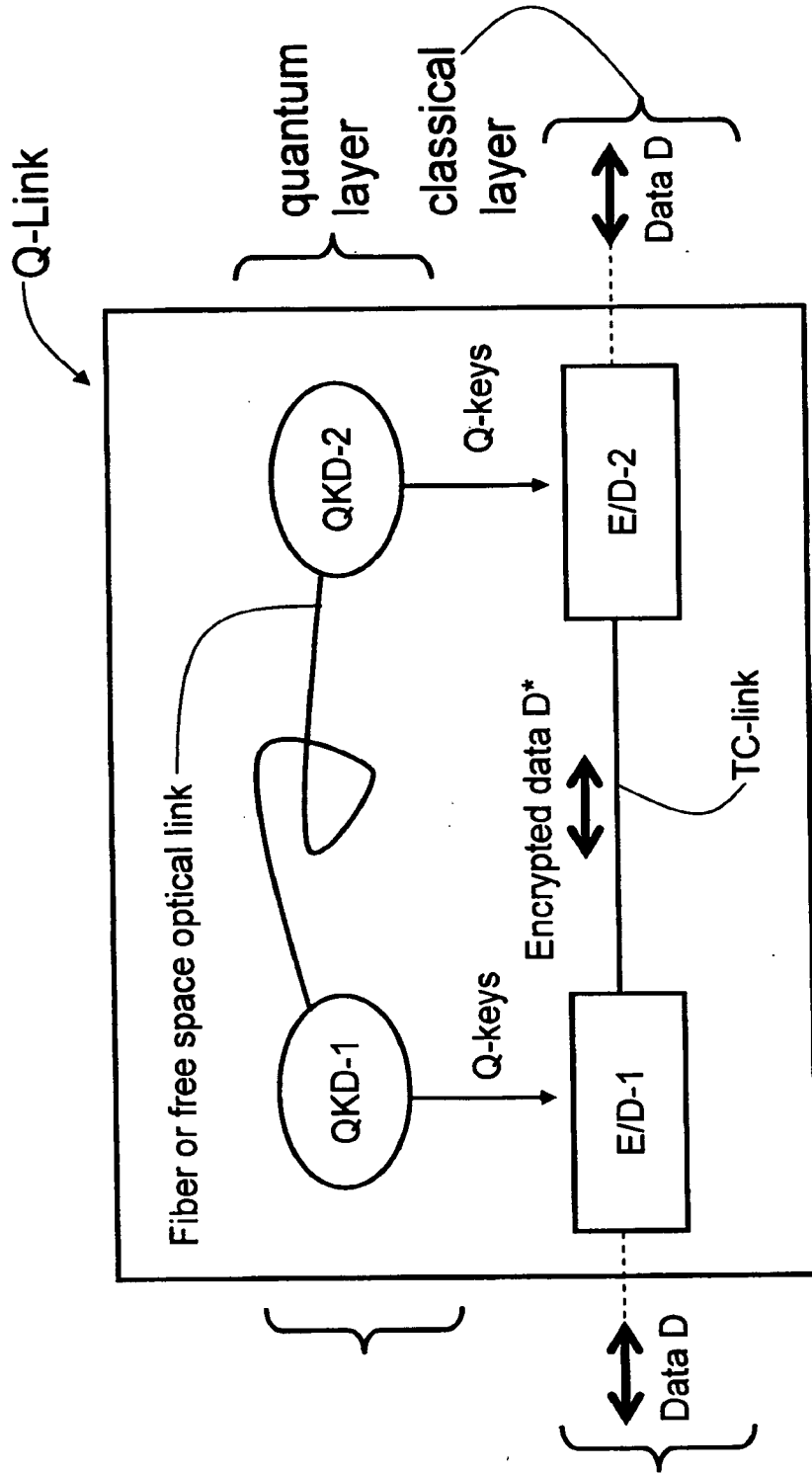


FIG. 1

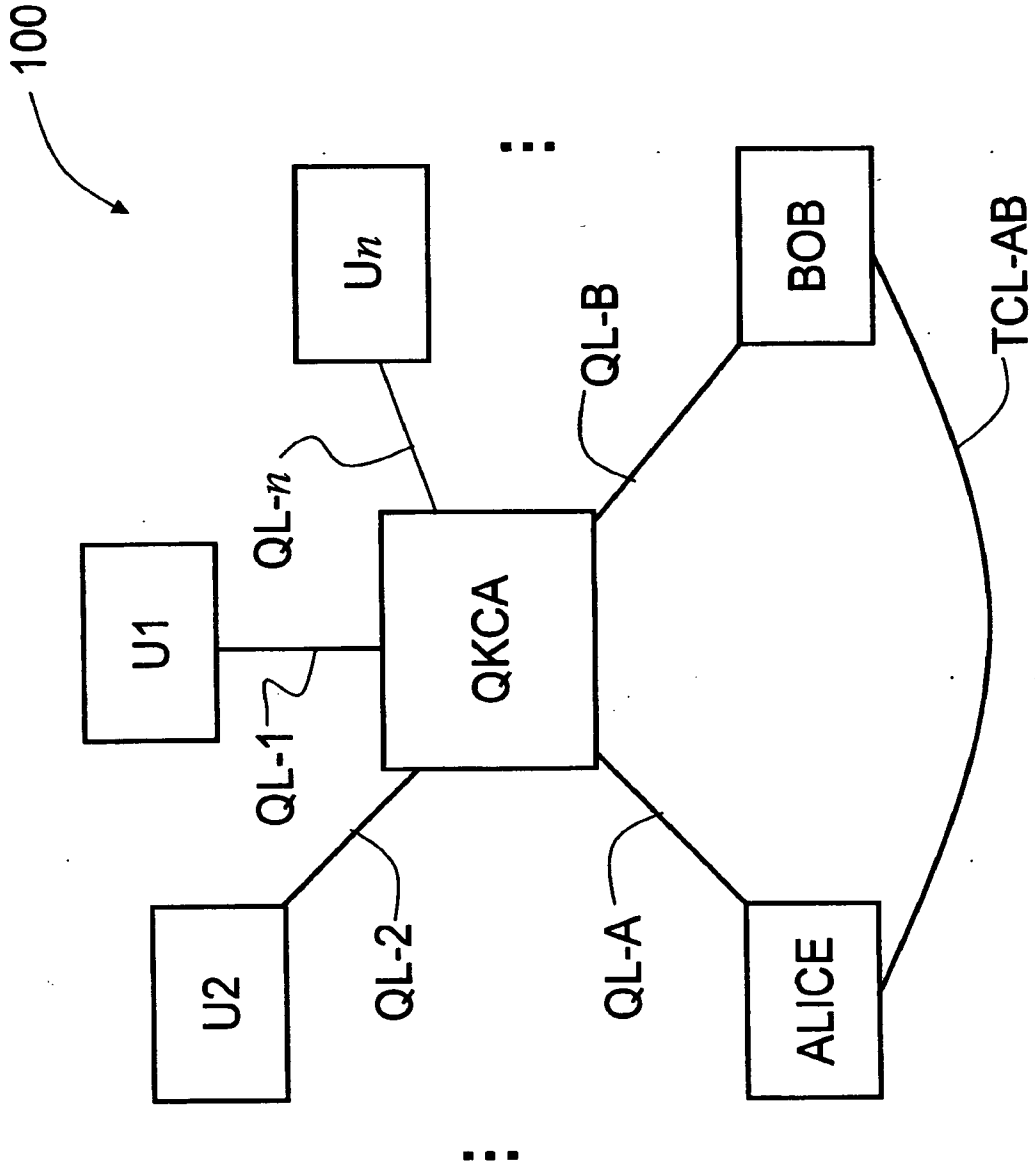


FIG. 2

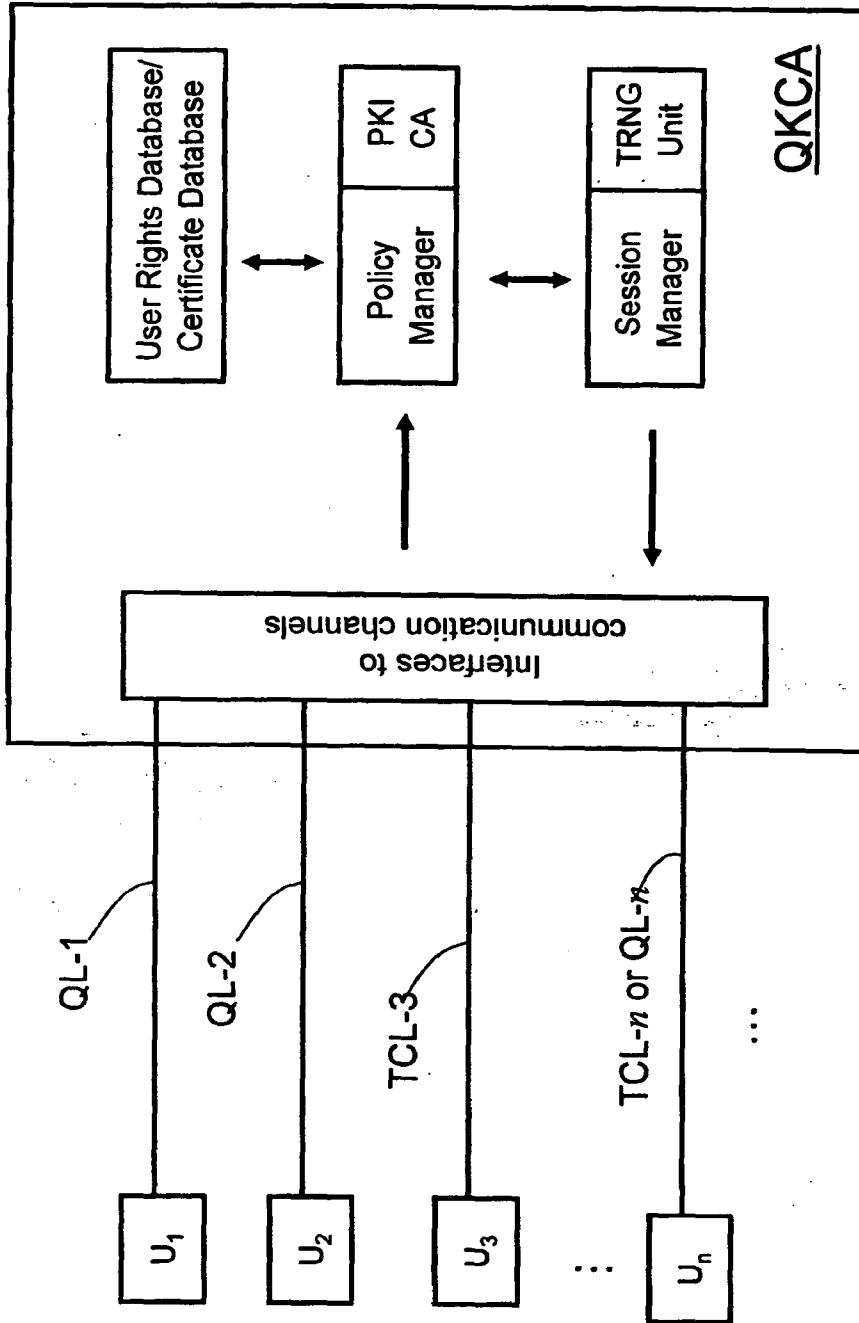


FIG. 3

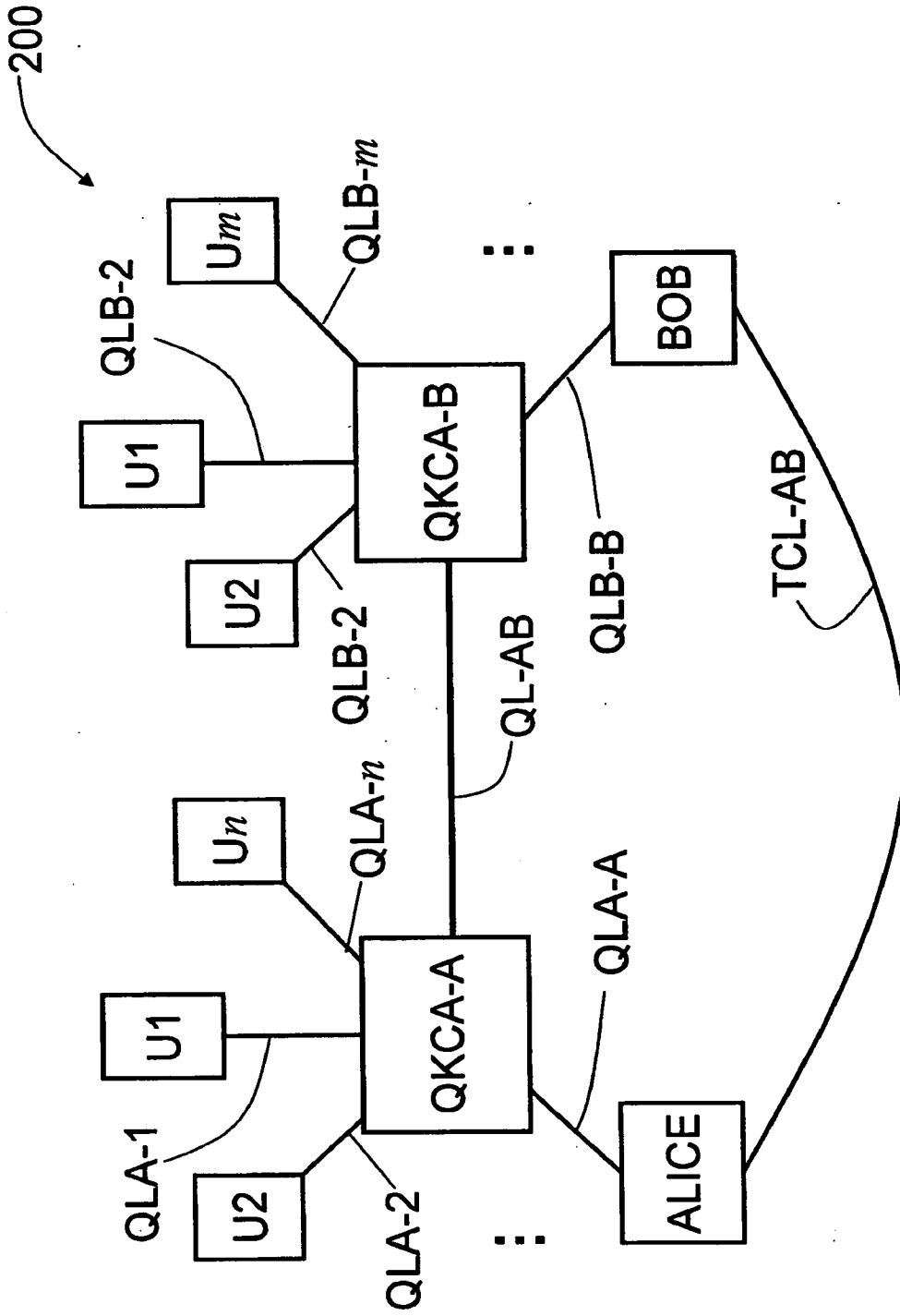


FIG. 4

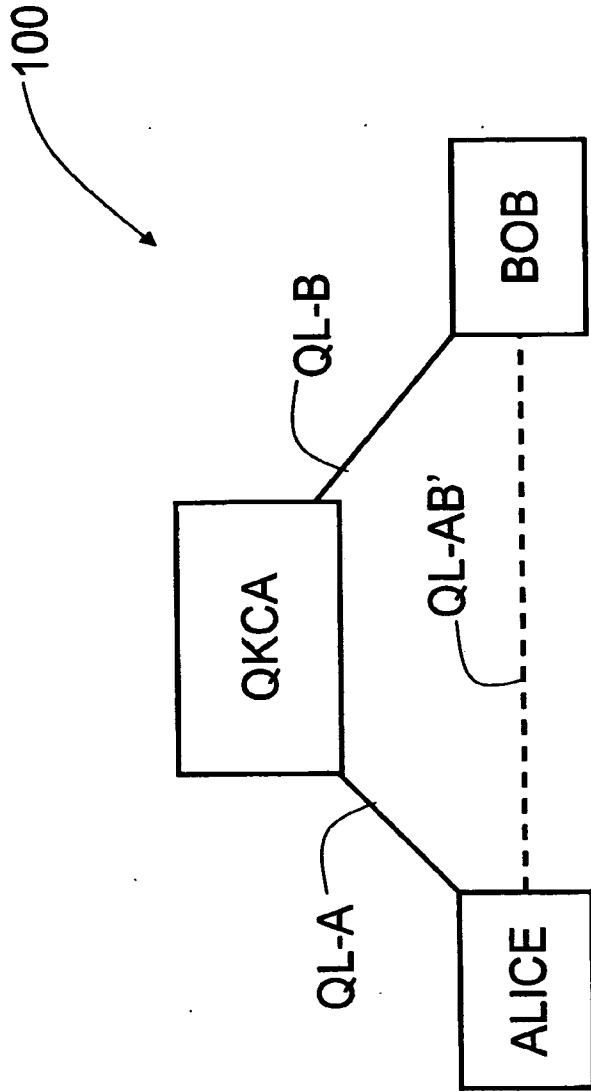


FIG. 5