(21) International Application Number: PCT/My2009/000999

(22) International Filing Date: 21 July 2009 (21.07.2009)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant (for all designated States except US): MIMOS BERHAD [MY/MY]; Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants (for US only): ISKANDAR, Bahari [MY/MY]; Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). MUSTAFA, Affandi Mat Nor [MY/MY]; Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY). NORZIANA, Jamil [MY/MY]; Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 57000 Kuala Lumpur (MY).

(74) Agent: MOHAN, K.; Adstra Intellectual Property Sdn Bhd, P.O. Box 43, Suite 2B, Level 7, Menara Dato Onn, Putra World Trade Centre, 45, Jalan Tun Ismail, 50480 Kuala Lumpur (MY).


(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, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, 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 (Rule 48.2(g))

(54) Title: QUANTUM NETWORK RELAY

(57) Abstract: A method for quantum network relay introduces a new protocol of relaying a key by using deterministic quantum key distribution for several parties. The number of key generated can be maintained from the beginning to the end and will not be affected by the number of nodes in the network. The method includes the steps of providing a short secret seed key (11) and expanding the seed key to a longer key (12) for generating the length which is to be used as the measurement basis (13). The length, L of the key is maintained during every transmission. The process continues until the receiver node (23) receives L number of qubits.
Quantum Network Relay

Field of Invention

The present invention relates generally to quantum key-distribution and more particularly to a quantum relay method in term of key generation.

Background of the Invention

Quantum key distribution involves establishing a key between a sender ("Alice") and a receiver ("Bob") using weak optical signals or "qubits" transmitted over a "quantum channel". The security of the key distribution is based on the quantum mechanical principle that any measurement of a quantum system in unknown stage will modify its state. As a consequence, an eavesdropper ("Eve") who attempts to intercept or otherwise measure the qubits will introduce errors and reveal her presence.

One of the limitations in quantum key distribution (QKD) is the distance where the existing technology claims it can only go up to 122km. This is because of the usage of weak single photon and the problem of noisy quantum channel that introduce disturbance and errors. The currently available quantum cryptographic techniques, are based primarily on the well-
known Bennett-Brassard (BB84) techniques that have many limitations namely its inefficiency and impractical use for long-distance or network communications.

There are other different approaches proposed to extend the distance of QKD and one of them introduces the idea based on the well-known intercept or resend eavesdropping strategy and known trusted quantum relay. In the protocol, a new node is introduced to act like Eve is doing an intercept or resend attack so that the distance between Alice and Bob is doubled. It can also be implemented for multiple nodes \( (n) \) system for longer distance. The protocol is shown to be secured from eavesdropping but the weakness of this technique is on the efficiency. By using a non-deterministic protocol to generate a key between nodes, the key generated is reduced by half for each new node introduced. The efficiency decreases with the increasing number of nodes and the end party (Bob) can only received \( \frac{1}{2^n} \) bits of key which is very inefficient.

Research has also been made to realize quantum communication over a long distance by generating quantum systems having quantum correlation called an entanglement at a long-distance from each other.

Particular Quantum Key Distribution ("QKD") protocols such as BB84 enable secure key exchange between two devices by
representing each bit of a key with a single photon. Distribution of the quantum keys is secure because in accordance with the laws of quantum physics, an eavesdropper attempting to intercept the key would introduce detectable errors into the key since it is not possible to measure an unknown quantum state of a photon without modifying it.

The present invention has overcome the drawbacks of the existing methods and provides significantly improved and secured quantum network relay.

An objective of the present invention is to provide an efficient quantum key distribution method which realizes long-distance communication where the number of key generated can be maintained regardless of the number of intermediate nodes.

The present invention also seeks to provide an efficient scheme which is expected to solve the limitation when a deterministic quantum protocol is used to relay the key which provides a better key rate generation.

Yet another objective of the present invention is to provide the efficiency method which would have no limitation in the number of intermediate nodes within the network as the sustenance of key is maintained during every transmission.
Other objects of this invention will become apparent on the reading of this entire disclosure.

Summary of the Invention

In the present invention, a method for quantum network relay comprising the steps of providing a shared short secret seed key at each consequence node of the network, expanding the secret seed key to a longer key for generating the length of

the longer key which is to be used as the measurement basis;

preparing a first qubit based on a first longer key from a sender node to be sent to a second node, measuring the qubit with reference to the same first longer key by the second node, where the second node then preparing a qubit based on the result of the measurement and a second longer key that it shares with third node, repeating the measuring qubit step with respective longer key by the third node and continues until it reaches receiver node, and restarting the first step for a second qubit by the sender node and the process continues until length number of qubits received by the receiver node.

Preferably the qubit prepared by the sender node based on the first longer key, \( R_i \) is based on the condition where \( R_i \) is a 0, the sender node prepares the qubit in a rectilinear state (0° or 90°) with 0° represents a '0' and 90° represents a '1', and
\( R_1 \) is a \( 1 \), diagonal (45° or 135°) polarization is used with 45° represents a '0' and 135° represents a \( \Lambda_1 \).

Preferably the short secret seed key, \( K_i \) is used repeatedly to produce the longer key, \( R_i \).

Preferably the short secret seed key, \( K_i \) is expanded through a pseudo-random number generator (PRNG).

10 Brief Description of the Drawings

Other objects, features, and advantages of the invention will be apparent from the following description when read with reference to the accompanying drawings. In the drawings, wherein like reference numerals denote corresponding parts throughout the several views:

Figure 1 shows a flow chart of the quantum network relay scheme of the present invention.

20 Detailed Description of the Preferred Embodiments

In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those of ordinary skill in the art that the invention may
be practiced without these specific details. In other instances, well-known methods, procedures and/or components have not been described in detail so as not to obscure the invention. Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings.

In a standard quantum communication system, the system includes a first channel station used by a first user, designated "Alice" hereinafter and a second channel station used by a second user, designated "Bob" hereinafter, linked by a communication link. It is conventional to refer to the two communicating parties, sender and receiver in quantum key distribution (QKD) as "Alice" and "Bob", respectively and to a potential eavesdropper as "Eve". In the present invention, the quantum communication system has a new protocol of relaying a key by using a deterministic quantum key distribution for several parties. The relay is basically using the well-known intercept/resend eavesdropping scheme, however with a variant to deterministic protocol, the system has increases the efficiency of quantum relay system in term of key generation. In the present invention, the secure deterministic quantum scheme having a protocol which allows for the use of privacy amplification in noisy channels where Alice is sending predetermined strings rather than generating random ones.
The preferred embodiment of the present invention is a deterministic quantum scheme having a protocol of relaying a key for several parties. Alice is assumed at node 1 and Bob at node n. An N number of relay stations are located between Alice and Bob as intermediate nodes. Each node is assumed sharing a short secret seed key $K_i$ with its consequence node where $i = 1, 2, \ldots, n$ (11) as shown in figure 1. The secret seed key, $K_i$, is either to be used repeatedly or expanded through a pseudo-random number generator (PRNG) (12) to produce a longer key $R_i$, which is to be used as the measurement basis (13).

In the first method, a secure random sequence (the bases sequence) determines the encoding bases in the scheme. Eve is prevented from knowing about the encoding bases as she does not know the bases sequence. The public announcement of the bases is not needed and it means that Eve cannot distinguish which basis is used and that the bases sequence can be used repeatedly. When the bases sequence can be used repeatedly the key can be distributed many times.

In the second method, where the secret seed key, $K_i$, is expanded through a pseudo-random number generator (PRNG), let $f^k$ be the quantum state corresponding to data sequence $x = x_1 \ldots, X_n$ and longer key $k_i \ldots, k_n$. By an optimal measurement on the qubits,
Eve's probability of correctly identifying \( k \) and then \( K \) may be obtained via \( \mu^k \). In this method, the secret seed key, \( K_i \) is applied to a standard encryption mechanism to generate a random extended key \( R_i \) which is applied to a modulator for encrypting the data \( X \). The encrypted data is transmitted via an optical communication channel to the receiver Bob. At Bob, the secret seed key \( K_i \) is applied to a standard encryption mechanism to generate the same random extended key \( R_i \) for a demodulator for decrypting the encrypted data \( X \).

The length \( L \) of \( R_i \) is dependent on the size of key to be generated. Alice who is at node 1, then prepares a qubit based on \( R_i \) (14). If \( R_i \) is a 0 (15), Alice prepares the qubit in a rectilinear state (0° or 90°) where 0° represents a \( \Lambda_0' \) and 90° represents a \( \Lambda_1' \) (16). And if \( R_i \) is a 1 (17), diagonal (45° or 135°) polarization is used where 45° represents a \( \Lambda_0' \) and 135° represents a \( \Lambda_1' \) (18). Alice then sends the qubit to node 2 (20). With reference to the same \( R_i \), the node measures the qubits accordingly (19) where if \( R_i \) is 0, the rectilinear basis is used or otherwise. Based on the result of the measurement and \( R_2 \) that it shares with node 3, node 2 prepares a qubit in the same way as Alice prepared the qubit based on \( R_i \) at node 1 (21).
Node 3 repeats steps (19) and (21) with respective \( R_j \) and the process continues until it reaches node \( n \) (Bob) (22). Alice restarts step (11) for the second qubit and the whole process continues until the length, \( L \) number of qubits received by Bob (23). The original length, \( L \) of the key is maintained at the receiver end, Bob regardless to the number of intermediate nodes, therefore there are no limitation in the number of intermediate nodes within the network since the substance of key is maintained during every transmission. Alice and Bob then proceed with the estimation of error, error correction and privacy amplification (24) to obtain a secret key. The deterministic protocol to relay the key in the present invention provides a better key rate generation.

Privacy amplification phase is used after error correction phase. In a quantum key distribution (QKD) setup, we can imagine the execution of error correction procedures, of which after that, Eve still has substantial information of the key. Privacy amplification is a procedure that allows two parties to distill a secret key from a common random variable about which the eavesdropper (EVE) has partial information. The privacy amplification has the effect of shrinking the key while eliminating Eve's information of the key.

As will be readily apparent to those skilled in the art, the present invention may easily be produced in other specific
forms without departing from its essential characteristics. The present embodiments is, therefore, to be considered as merely illustrative and not restrictive, the scope of the invention being indicated by the claims rather than the foregoing description, and all changes which come within therefore intended to be embraced therein.
Claims

1. A method for quantum network relay comprising the steps of:
providing a shared short secret seed key at each consequence node of said network (11);
expanding said secret seed key to a longer key for generating the length of said longer key (12) which is to be used as the measurement basis (13);
preparing a first qubit based on a first longer key (14) from a sender node to be sent to a second node (20);
measuring the qubit with reference to the same first longer key by said second node (19), where said second node then preparing a qubit based on the result of the measurement and a second longer key that it shares with third node (21);
repeating said measuring qubit step (19, 21) with respective longer key by said third node and continues until it reaches receiver node (22); and
restarting the first step for a second qubit by said sender node and the process continues until the length number of qubits received by said receiver node (23).

2. The method for quantum network relay as claimed in claim 1, wherein said qubit prepared by said sender node (14) based on said first longer key, R1 is based on the condition where:
$R_i$ is a 0 (15), said sender node prepares the qubit in a 
rectilinear state (0° or 90°) with 0° represents a '0' and 90°
represents a '1' (16); and

$R_i$ is a 1 (17), diagonal (45° or 135°) polarization is used 
with 45° represents a '0', and 135° represents a '1' (18).

3. The method for quantum network relay as claimed in claim 1,
wherein said the length, L of the longer key is dependent on 
the size of the key to be generated.

4. The method for quantum network relay as claimed in claim 3,
wherein said length of the key is maintained at the receiver 
node regardless of the number of intermediate nodes.

5. The method for quantum network relay as claimed in claim 1,
wherein said short secret seed key, $K_i$ is used repeatedly to 
produce said longer key, $R_i$, (12).

6. The method for quantum network relay as claimed in claim 1,
wherein said short secret seed key, $K_s$ is expanded through a 
pseudo-random number generator (PRNG) (12).

7. The method for quantum network relay as claimed in claim 1,
wherein said method further comprising the step of performing 
the estimation of error, error correction and privacy 
amplification to obtain s secret key (24).
Start

Node $i$ has already shares a short secret key $K_i$ with node $i+1$. ($i = 1, 2, ..., n$)

$K_i$ is arranged repeatedly or expanded via a PRNG

A running key $R_i$ with length $L$ for basis determination

Node $i$ prepares a qubit based on $R_i$

11

12

13

14

$R_i = 0$?

Yes

The qubit is polarized at 45° to represent a '0' or at 135° to represent a '1'.

Node $i+1$ measures the qubit based on the $R_i$.

Node $i$ sends the qubit to node $i+1$

15

No

The qubit is polarized at 0° to represent a '0' or at 90° to represent a '1'.

16

17

18

Node $i+1$ measures the qubit based on the $R_i$.

Node $i$ sends the qubit to node $i+1$

19

20

21

$i = i + 1$

22

$i > n$?

No

Yes

$i = i + 1$

23

24

Reset $i = 1$

Node 1 and node $n$ execute error estimation, error correction and privacy amplification

End

Figure 1