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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2011 (06.01.2011)

PCT

(10) International Publication Number
WO 2011/002276 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/MY2010/000114

(22) International Filing Date:
30 June 2010 (30.06.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI20092759 29 June 2009 (29.06.2009) MY

(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)*: **EL-ORANY, Faisal Aly Aly** [CZ/CZ]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 5700 Kuala Lumpur (MY). **WAHIDDIN, Mohamed Ridza** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 5700 Kuala Lumpur (MY). **MAT NOR, Mustafa Afanddi** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 5700 Kuala Lumpur (MY). **JAMIL, Norziana** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 5700 Kuala Lumpur (MY). **BAHARI, Iskandar** [MY/MY]; c/o Mimos Berhad, Technology Park of Malaysia, Bukit Jalil, 5700 Kuala Lumpur (MY).

(74) Agent: **MOHAN, K.**; Adastra Intellectual Property Sdn Bhd, A-28-10 Menara UOA Bangsar, N°5 Jalan Bangsar Utama 1, 59000 Kuala Lumpur (MY).

(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, 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, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, 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, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, 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, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

[Continued on next page]

(54) Title: QUANTUM KEY DISTRIBUTION IN TERMS OF THE GREENBERGER-HORNE-ZEILINGER STATE - MULTI-KEY GENERATION

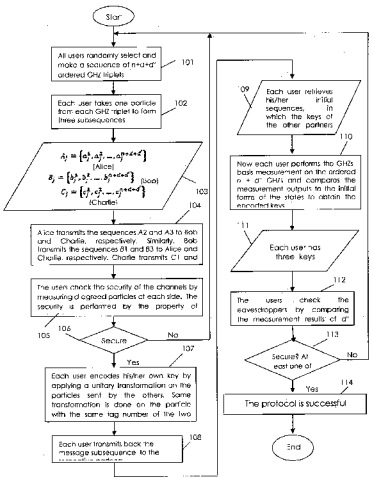

FIG. 1

(57) Abstract: The present invention provides a method of carrying out communication between multiple users based on quantum key distribution (QKD). The method comprises generating (101) Greenberger-Horne-Zeilinger states (GHZs) by all users randomly; distributing (102) a particle from each GHZs to form sub-sequences; forming (103) a plurality of sequences correspond to a plurality of users based on the particles on each user, wherein one of the sequences generated by the sender comprises a home sequence; transmitting (104) to the each other users a separate sequence; checking (105) security of the channels through verifying the sequences; encoding (107) users' own key that are in the particles of the other users; transmitting (108) blocks of particles back to the corresponding user; retrieving (109) own initial sequences, wherein the keys of the other users are decoded; performing (110) a GHZs measurement to obtain encoded keys by each user; and comparing (112) the measurement results at each user site.

WO 2011/002276 A1

— *the filing date of the international application is within two months from the date of expiration of the priority period (Rule 26bis.3)*

Quantum Key Distribution in Terms of the GreenBerger-Horne-Zeilinger State – Multi-Key Generation

Field of Invention

The present invention is related to quantum cryptography. Precisely, it provides a method to carry out quantum key distribution between multiple users via Greenberger-Horne-Zeilinger states.

Background of the Invention

Quantum cryptography is one of the most fruitful applications in the quantum information theory. Among others, quantum key distribution (QKD) is a method allowing two or more legitimate users of a communication channel to establish two or more exact keys. This will be in the form of a random and secret sequence of bits. The advantage of the quantum cryptography over the classical one lies in the following: the former follows the quantum laws, e.g., the Heisenberg uncertainty principle, no-cloning theorem and the quantum correlations, to protect the distribution of the cryptographic keys. Therefore, the message and the key are secure since the legitimate users can easily detect the eavesdroppers. Various protocols have been developed in the framework of the quantum cryptography. Most of these protocols follow the original three constructs, namely, the BB84 protocol, the B92 protocol and the EPR protocol.

Entanglement is one of the main ingredients in the quantum information theory. Based on this property, various protocols have been developed. The known "ping-pong" protocol has been given to achieve deterministic direct communication between the legitimate users. This protocol has advantages and disadvantages; it allows the transmission of either a

secret key or the plaintext message. Nevertheless, it is insecure (quasi-secure) when it is operating in a noisy (perfect quantum) channel.

In the entanglement protocols, the Einstein-Polosky-Rosen state (EPR) has been used to distribute the quantum-cryptographic key. The security has been checked either by the violation of the Bell inequalities or by the correlation of the EPR. Furthermore, Greenberger-Horne-Zeilinger states (GHZs) have been already involved in the quantum cryptography. These states are distinguished by a large Hilbert space compared to the EPR. In the GHZs protocols one can have two or more legitimate users. In the two users case, the distribution of the GHZs particles and the quantum states are asymmetrical between the users, hereinafter referred to as Alice and Bob. Additionally, the security can be established via the correlation of the GHZ triplet state, as illustrates in G. Zeng quant-ph/0001044, for example. In the multi-user case, say three users, which include a sender, a recipient and supervisor. The supervisor controls the entanglement and information transmission between the sender and the recipient. The users can get the key only by joint cooperation. In this respect, the protocol is secured against the dishonest user (if one exists).

The GHZs has been used in the quantum secure direct communication and in the teleportation, too. It is worth mentioning that the simultaneous quantum direct communication between users based on the GHZs has been developed by X.-R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, C.-I. Um, Phys. Lett. A 354 (2006) 67. However, it is shown in F. Gao, S.-J. Qin, Q.-Y. Wena and F.-C. Zhuc Physics Letters A 372 (2008) 3333–3336 that this protocol is not secure. Finally, the GHZs has been experimentally implemented by various means, e.g., using entanglement swapping starting from three down converters (as of M. Zukowski, A. Zeilinger, H. Weinfurther, Ann. N.Y. Acad. Sci. 755 (1995) 91), using two pairs of entangled photons (as of D. Bouwmeester, J.W. Pan, M. Daniell, H. Weinfurther, A. Zeilinger, Phys. Rev. Lett. 82 (1999) 1345), based on dipole-

induced transparency in a cavity-waveguide system (as of J. Qian, Y. Qian, X.-L. Feng, T. Yang, S.-Q. Gong, Phys. Rev. A 75 (2007) 032309), in the framework of the superconducting circuits (as of L. F. Wei, Yu-xi Liu, F. Nori, Phys. Rev. Lett. 96 (2006) 246803) and nuclear magnetic resonance (as of R. J. Nelson, D. G. Cory, S. Lloyd, Phys. Rev. A 61 (2000) 022106).

It can thus be seen that there exists a need for a robust way for a system and method to provide a more efficient and secure technique for communications between different users. This what we are going to show in this invention. The invention can be used in the banking system and military applications.

Summary of the Invention

The object of the present invention is to provide a quantum key distribution protocol adapted to produce more than one key at one round transmission. The protocol should be proceeded with at least one secure key. This avoids halting protocol after eavesdropper attacking. Moreover, the protocol is highly secure. This is based on the entanglement property, many keys generation and checking eavesdroppers at two stages of the protocol.

The present invention provides a method of carrying out QKD between multiple users via GHZs. The method comprises generating (101) sequences of Greenberger-Horne-Zeilinger states (GHZs) by all users randomly; distributing (102) particles from each GHZs to form sub-sequences; forming (103) a number of sequences correspond to the number of users, each user keeps one of the generated subsequences (home sequence) in his work station; transmitting (104) to the each other users a separate sequence; checking (105) security of the channels through comparing the measurement outcomes of the agreed-upon portion of the particles; encoding (107) users' own key that are in the particles of the other users; transmitting (108) blocks of particles back to the corresponding user; retrieving (109) own

initial sequences, wherein the keys of the other users are decoded; performing (110) a GHZs measurement to obtain encoded keys by each user; and checking (112) the purity of the keys by comparing the measurement results of the agreed-upon portion of particles at each side.

Brief Description of the Drawings

This invention will be described by way of non-limiting embodiments of the present invention, with reference to the accompanying drawing, in which:

FIG. 1 illustrates a process of quantum key distribution in accordance with one embodiment of the present invention.

Detailed Description of the Preferred Embodiments

In line with the above summary, the following description of a number of specific and alternative embodiments is provided to understand the inventive features of the present invention. It shall be apparent to one skilled in the art, however that this invention may be practiced without such specific details. Some of the details may not be described at length so as not to obscure the invention. For ease of reference, common reference numerals will be used throughout the figures when referring to the same or similar features common to the figures.

In this invention, a quantum key distribution protocol based on the Greenberger-Horne-Zeilinger states (GHZs) is provided. The particles are exchanged among the users in blocks through two steps. In this protocol, for three-particle GHZs three keys can be simultaneously generated. The advantage of this is that the users can select the most suitable key for communication. The protocol can be generalized to N users to provide N keys. The protocol has two levels for checking the eavesdroppers. Moreover, we discuss the security of the protocol against different attacks.

In one embodiment, the present invention provides a protocol using the GHZs. In particular, the protocol allows the communication between three or more legitimate users without any controllers. The number of the keys generated in this protocol depends on the number of the users and/or the number of particles in the GHZs. Typically, each key is generated for one user and/or particle in the GHZs.

In a set of the three-particle GHZs, for example, it includes eight independent states, which form a complete orthonormal basis as follows:

$$\begin{aligned} |\psi_1\rangle &= \tfrac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad |\psi_2\rangle = \tfrac{1}{\sqrt{2}}(|000\rangle - |111\rangle), \\ |\psi_3\rangle &= \tfrac{1}{\sqrt{2}}(|100\rangle + |011\rangle), \quad |\psi_4\rangle = \tfrac{1}{\sqrt{2}}(|100\rangle - |011\rangle), \\ |\psi_5\rangle &= \tfrac{1}{\sqrt{2}}(|010\rangle + |101\rangle), \quad |\psi_6\rangle = \tfrac{1}{\sqrt{2}}(|010\rangle - |101\rangle), \\ |\psi_7\rangle &= \tfrac{1}{\sqrt{2}}(|110\rangle + |001\rangle), \quad |\psi_8\rangle = \tfrac{1}{\sqrt{2}}(|110\rangle - |001\rangle). \end{aligned} \tag{1}$$

These states can be switched from one to another by applying one of the four unitary operators $\hat{I}^{(j)}, \hat{\sigma}_x^{(j)}, i\hat{\sigma}_y^{(j)}, \hat{\sigma}_z^{(j)}$, where the superscript j represents j^{th}-particle which is commonly used in the art. It is the main object in generating the keys. The users have to agree, in advance, about the following Boolean values:

$$\hat{I}^{(j)} \longrightarrow 0, \quad \hat{\sigma}_x^{(j)} \longrightarrow 1. \tag{2}$$

Sometimes, when applying two operations on the states $|\psi_j\rangle$ can give the same results as follows:

$$\begin{aligned} &\hat{I}^{(2)}\hat{I}^{(3)}|\psi_1\rangle = \hat{\sigma}_z^{(2)}\hat{\sigma}_z^{(3)}|\psi_1\rangle = |\psi_1\rangle \\ &\hat{\sigma}_x^{(2)}\hat{\sigma}_x^{(3)}|\psi_1\rangle = \hat{\sigma}_y^{(2)}\hat{\sigma}_y^{(3)}|\psi_1\rangle = |\psi_3\rangle \end{aligned} \tag{3}$$

Such situation is a weakness for decoding process, however, it is an advantages in the security framework of the present protocol because it confuses eavesdroppers.

FIG. 1 illustrates a process of quantum key distribution in accordance with one embodiment of the present invention. For illustration purpose, three users, Alice, Bob and Charlie are provided for simplicity, and it is understood that more users are possible. The

process starts with step **101**, where Alice prepares a sequence A of $n + d + d'$ ordered GHZ triplets, each of which forms (a_1^k, a_2^k, a_3^k), $k = 1, 2, ..., n + d + d'$ where the superscript k denotes the order of the triplet in the sequence A. These triplets are randomly chosen from the set given in (1), and are already known to Alice. At step **102**, Alice takes one particle $a1$; $a2$; $a3$ from each GHZ triplet to form three ordered particles sequences $A_j = \{a_j^1, a_j^2, ..., a_j^{n+d+d'}\}$ with $j = 1, 2, 3$ (at step **103**). Bob and Charlie, on their sites, do the same as Alice, i.e. takes one particle from each GHZ triplet to form three sub-sequences. In the case of Bob and Charlie, they have the sequences $B_j = \{b_j^1, b_j^2, ..., b_j^{n+d+d'}\}$ and $C_j = \{c_j^1, c_j^2, ..., c_j^{n+d+d'}\}$ with $j = 1; 2; 3$, respectively.

At step **104**, Alice transmits the sequences $A2$ and $A3$ to Bob and Charlie, respectively. Similarly, Bob transmits the sequences $B1$ and $B3$ to Alice and Charlie, respectively and Charlie transmits $C1$ and $C2$ to Alice and Bob respectively. The sender is informed, via classical channels, before the transmission and the receivers should confirm the reception of the particles. This process is used to avoid unwanted circumstances under which Eve (possible eavesdropper) can impersonate one or both of the users. The transmission of the particles occurs in blocks and the orders of the sequences are not known for the receivers. The arrangement would increase the security of the present protocol.

At step **105**, the users check the security of the channels to see if there is any the eavesdropper within the communication, which is independently carried out for each sequence. In the case of Alice's sequence $A = (A1;A2;A3)$, Bob may have chosen randomly a large subset d of particles from the sequence $A2$ and measures each of them using one of the two bases x or z. Then Bob publicly tells Alice and Charlie via a classical channel about the positions, the basis and the measurement outcome for each of the particles. Charlie, using the same bases, measures the corresponding particles from the sequence $A3$, and publicly tells the

others about the results. After that Alice applies the same procedure for the particles in the home sequence $A1$.

Consequently, at step **106**, the users decide whether eavesdroppers are within the communication. If the measurement outcomes are different, then Eve (or eavesdropper) is determined not within the communication, and vise versa. Similar procedures have to be executed for the sequences $\{B1;B3\}$ and $\{C1;C2\}$. At this step, there is no need to evaluate the error rates since the keys have not been generated yet. The user with the home particles, i.e. Alice, should be the last one executing eavesdropper checking for the set d. This, in turn, helps in finding out the unauthorized user, if any.

At step **107**, each partner would have his own key for transmitting to the others. Each partner encodes his own key in the particles of the other partners by means of the operations shown in equation (2). Each also uses one operator to act simultaneously on the two particles from the different sequences, however, in the same order. For instance, suppose that Alice wants to encode the bits 1 in the j^{th}-particle for the other partners. In this case, she should act by $\hat{\sigma}_x^{(j)}$ on the j^{th} particle in the sequences $B1$ and $C1$. The similar procedures are carried out on Bob and Charlie sites. During the encoding process the users should be careful regarding the information and the positions of the particles of the set d'. The reason is that the users will sacrifice these particles when checking the eavesdroppers in the final step.

At step **108**, the encoding process ends and each user transmits the blocks of particles (message particles) back to the other partners. The parties are informed prior to the transmission and after the reception of the blocks. At step **109** the users obtain their original particles, in their new form. For instance, Alice, after a successful transmission, has the sequence $A = \{(a_1^1, a_2', a_3'), (a_1^2, a_2'^2, a_3'^2), ..., (a_1^{n+d'}, a_2'^{n+d'}, a_3'^{n+d'})\}$, where the dash means that these particles are different from the original ones since now they carry the keys. The sequences

$\{a_2^{'j}, j = 1, ..., n + d'\}$ and $\{a_3^{'j}, j = 1, ..., n + d'\}$ include Bob and Charlie keys, respectively, and the sequence $\{a_1^j, j = 1, ..., n + d'\}$ is the home sequence. As Alice prepared these particles initially she knows them very well. At step **110**, Alice then performs the GHZs measurement on the ordered $n + d'$ GHZs and compares the measurement outputs with the initial forms of the states to obtain the keys of Bob and Charlie. For instance, if Alice initially prepared one of the triplets in the state $|\psi_1\rangle$ and the measurement result is $|\psi_3\rangle$. From equations (1) and (2), Alice has the relation $|\psi_3\rangle = \hat{\sigma}_x^{(2)}\hat{\sigma}_x^{(3)}|\psi_1\rangle$. According to the equation (2), Alice knows with certainty that Bob and Charlie bits are 1 and 1, respectively, and so on. At the same time Bob and Charlie perform the same procedures of the steps **109** and **110**, for which, at step **111**, each user would obtain three keys, i.e. one own key and two keys for the others in the communication. At this moment there is no overlap between the users since each one has retrieved his own sequence of the GHZs in its new forms. Thus they cannot check the eavesdroppers based on the entanglement property as provided in C. H. Bennett, G Brassard, N. D. Mermin, Phys. Rev. Lett. 68 (1992) 557 10. In this case, the users can use the virtue of the set d'.

At step **112**, the senders know the positions of the particles of the set d' and the information included. They designed their keys based on the bits provided by these particles which are excluded from the generic keys. For illustration of this scenario, the set d' of Alice is provided therein below, the rest shall be applied accordingly. Alice publicly informs Bob and Charlie via a classical channel about the set d', i.e. the positions of the particles and the bases which should be used for the measurement but not the results. Bob and Charlie follow Alice's prescription and they announce the measurement results sequentially, i.e. Bob announces the measurement of the first particle, then Charlie the second one, then Bob and so on. Such process is sufficient to detect any dishonest user, if present. If there are overlaps

between the results of the measurements then the key is secured, which otherwise they should evaluate the error rate for this key. Then the users should follow the same steps for the sequences *B* and *C*. Comparison among these three error rates drives the users to choose the most suitable key for the communication. Moreover, based on the positions of the particles in the set *d'* the users can bring some diversions to delude Eve, i.e. by using particular types of swapping entanglement and/or shifting process for the bits of the final keys. Nevertheless, they should agree in advance.

At step **113**, when the communication is determined as secured, the communication between the users are considered successful at step **114**. If the communication is determined to be unsecured, the present protocol is restarted from step **101**.

In another embodiment, the protocol can be extended to *N* parties. In this case, at the end of the protocol, the users obtain *N* keys. Each user generates a sequence of *N* particles in the GHZs, which has the form:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|j_1 j_2 \cdots j_N\rangle + |j_1' j_2' \cdots j_N'\rangle), \qquad (4)$$

where $j_p, j_p', (p = 1, \ldots, N)$ are bits 0 or 1 according to the specified states. The users should follow the same steps generally discussed above. The users obtain the generic key by making a comparison among the *N* keys. The larger the numbers of the keys, the higher the probability of obtaining a secured key because it would be difficult for Eve to efficiently attack many keys at the same time. She is vulnerable enough at least for one of the keys.

In view of the foregoing, the present protocol provides two levels of security, i.e. before and after the encoding process. Generally, Eve will only be able to get information on the keys if she manages to obtain information about the particles before and after the encoding process. This, of course, requires that the users did not detect her in the step **105**.

In another scenario, for example, suppose that Eve managed to attack the traveling particles without disturbing the channels, i.e. a double-CNOT attack, the mutual information between different users are unity, i.e., $Iij = 1$ where $i; j = A;B;C;E$. If the users are going to use only a message authentication as a security strategy, they would never be able to detect the double-CNOT attack. Generally, the double-CNOT attack mechanism includes, in a forward path, Eve performs a first CNOT gate between the particles in transit from Alice to Bob and to Charlie (control qubits) and her ancillae (target qubits). The second CNOT gate is executed in a backward path. In a case of Alice's particles, the scenario of the 2CNOT attack includes Alice keeping the first particle in her site and sending the second and third ones to Bob and Charlie, respectively. Eve executes her ancillae $|0\rangle_2^E|0\rangle_3^E$ with the transit particles and performs the first CNOT gate as:

$$U_{cont}(|\psi_1\rangle|0\rangle_2^E|0\rangle_3^E) = |\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle_2^E|0\rangle|0\rangle_3^E + |1\rangle|1\rangle|1\rangle_2^E|1\rangle|1\rangle_3^E). \quad (5)$$

It is obvious that the CNOT gate creates an entangled state composed from the traveling qubits and the Eve's ancillae. Suppose that Bob and Charlie act, respectively, by $\hat{I}^{(2)}$and $\hat{\sigma}_x^{(3)}$ on their corresponding particles according to their own keys. Thus,

$$\hat{I}^{(2)}\hat{\sigma}_x^{(3)}|\Psi_1\rangle = |\Psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|0\rangle_2^E|1\rangle|0\rangle_3^E + |1\rangle|1\rangle|1\rangle_2^E|0\rangle|1\rangle_3^E). \quad (6)$$

In the backward path Eve executes the second CNOT gate, which leads to:

$$U_{cont}(|\Psi_2\rangle) = |\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle)|0\rangle_2^E|1\rangle_3^E = |\psi_7\rangle|0\rangle_2^E|1\rangle_3^E. \quad (7)$$

It is evident that the generic state is flipped, i.e. $|\psi_1\rangle \longrightarrow |\psi_7\rangle$. In addition, the generic state and the Eve ancillae are disentangled. For Eve, it is enough to measure these ancillae in the z basis to get the information. To some extend, it is sufficient for Eve to obtain information regarding the keys. Eve cannot know the forms of the generic backward states since she would not be able to access the home particles. If Eve knows the Boolean relations from equation (2), then she may be able to obtain the keys. Such non-entangled protocol was

discussed in M. Lucamarini, S. Mancini, Phys. Rev. Lett. 94 (2005) 140501 for which the double-CNOT attack is reasonably efficient. Generally, Eve does not know any information about regarding the equation (2) and hence Eve should take into account the actions of the operators $\hat{\sigma}_z^{(j)}$ and $i\hat{\sigma}_y^{(j)}$. In this regard, the probability to get the key from this protocol, via the double-CNOT attack, is 25%, since the applied operation could be, e.g., one of the set from $\{\hat{I}^{(2)}\hat{I}^{(3)}, \hat{I}^{(2)}\hat{\sigma}_z^{(3)}, \hat{\sigma}_z^{(2)}\hat{I}^{(3)}, \hat{\sigma}_z^{(2)}\hat{\sigma}_z^{(3)}\}$. Accordingly, this indicates that the double-CNOT attack cannot give Eve valuable information about the keys.

The mechanism of this attack can be explained for Alice's particles as follows. In the forward path, Alice transmits the particles to Bob and Charlie, Eve blocks the particles, stores them in the memory and sends instead her particles to Bob and Charlie. In the backward path, i.e. Bob and Charlie transmit the particles back to Alice, Eve measures these particles to get the encoded information. At this moment Eve encodes the same information in the stored particles and passes them back to Alice. This is a dangerous attack, in particular, when Eve has full control of the classical channel. The solution against this kind of attack is that the legitimate users should share a prior secret letting them authenticate the channel and make it reliable when they communicate before and after the transmission processes. For the present protocol under such consideration, such attack is not helpful for Eve, where the users can detect her through the forward path in the step **105** with high probability. For instance, suppose that Alice uses the state $|\psi_1\rangle$, where she keeps the first particle with her and sends the second and third particles to Bob and Charlie, respectively. Eve has two possibilities for choosing ancillae, namely, GHZs and z basis states. If Eve uses one of the GHZs as a faked state, according to the set provided in equation (1), Eve has a probability of 1/8 to use the correct states. In this case, she has a probability of 1/3 to keep the correct particle with her pretending to be Alice. In this case, the probability that Eve may not be revealed in the step

105, is 1/24. On the other hand, if Eve is not on the communication, the measurements of the users in a control run (for the state $|\psi_1\rangle$) yield $|000\rangle$ and $|111\rangle$ with equal probability. Suppose that Eve uses the faked states from the z basis states, and if Eve qubits are one pair of the set $\{|0\rangle_B|0\rangle_C, |1\rangle_B|1\rangle_C\}$, where the subscripts B and C represent that these particles are sent to Bob and to Charlie, respectively, the measurement results corresponding to these ancillae are $\{(|000\rangle, |100\rangle), (|011\rangle, |111\rangle)\}$. Thus Eve will be detected, because her eavesdropping introduces an error rate equal to 1/2. When Eve's ancillae are one pair of the set $\{|0\rangle_B|1\rangle_C, |1\rangle_B|0\rangle_C\}$, the users would detect Eve with certainty. It illustrates that the present protocol is secured against double-CNOT attack.

In yet a further scenario, information leakage attack provided in F. Gao, S.-J. Qin, Q.-Y. Wena and F.-C. Zhuc Physics Letters A 372 (2008) 3333–3336 includes in some of the GHZ protocols, for example this that discussed in X.-R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, C.-I. Um, Phys. Lett. A 354 (2006) 67, the users obtain the keys only when Alice announces publicly its initial and final states. Thus Eve can easily obtain these results, and through comparing these results, Eve may obtain the keys. It has been illustrated in F. Gao, S.-J. Qin, Q.-Y. Wena and F.-C. Zhuc Physics Letters A 372 (2008) 3333–3336 that Eve can obtain three bits through the transmitted four bits. As the present protocol does not include such announcements and hence it is secure against this type of attack. We conclude by referring to the intercept-and-resend and disturbance attacks. The discussion is quite similar to that in X.-R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon,C.-I. Um, Phys. Lett. A 354 (2006) 67.

The same could be applied in the scenario when the security of the ping-pong protocol against considerable quantum channel losses that was discussed earlier. The present protocol can be treated in a quite similar way. This is based on the fact that it is enough for her to attack one of the traveling sequences of each users, e.g. $A2;B1;C3$. If the attention is focused

on one qubit of each sequence, the treatment will be the same as that of the ping-pong protocol.

The present protocol is based on the entanglement property of the GHZs. During the communications, the users (authorized) of the communication would have many keys so that they can choose the relevant one to establish the communication. There is no announcement about the forms of the states used in the present protocol and this improves the efficiency of the QKD. The proposed protocol includes a forward process where the senders transmit blocks of particles to the receivers, who encode the keys with the particles and transmit them back (backward process) to the senders. Eavesdroppers are checked in also two stages. For protocols operating via entanglement, the secret information is encoded in the whole entangled state. Therefore, Eve would not be able to obtain useful information if Eve has obtained only a part of the entangled state. Eve also cannot access the particles of the home sequences, i.e., the particles of $A1;B2;C3$.

Further, block-data transfer among the users as provided by C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, G. L. Long, Phys. Rev. A 71 (2005) 044305 too has various basic differences between the present protocol and the others. Firstly, the legitimate users can simultaneously generate various keys. Each user does not need the cooperation of the other users to obtain these keys. Eavesdroppers can be checked in the two stages under the protocol, which makes the protocol more secure.

X. R. Jin, X. Ji, Y.-Q. Zhang, S. Zhang, S.-K. Hong, K.-H. Yeon, C.-I. Um, Phys. Lett. A 354 (2006) 67, has disclosed the simultaneous quantum direct communication between users based on GHZs. Under the present protocol, the users obtain the messages only when Alice (sender) announces publicly the forms of the initial and final states under the present protocol. With this announcement, Eve can obtain most of the messages without using potential attacks. It is enough for her to compare the initial and final states. Suck

attack is known as information leakage attack. The present protocol is secured against information leakage attack, among others. The general differences between previous protocol and the current one are summarized in the table below.

Types/protocol	**Known Protocols**	**Present Protocol**
Input	one group of GHZs	three groups or more of GHZs
Output	one key	three keys or more
Users assistance	Needed	not needed
After attacking	Protocols stop	Protocol continues
Key owners	Two of the users	All users

Generally, most of the protocols in the existing art generate only one key for the users, which can be attacked by the eavesdroppers, and hence the protocol should be halted. The users need an assistance of each other to obtain the key. When comparing with BB84 protocol, it is observed that the present protocol is deterministic, multi-key generation, two ways communication, entanglement, and it is adapted to allow more than three communication parties. When comparing with E91 that based on the Bell states, the present GHZs based protocol provide three or more keys for more than three communication parties. Similarly, when comparing with ping pong protocol which is also based on a Bell states, the present GHZs based protocol also provide multiple key generations with data lock transfer, thus more secure. Yet, when comparing with the method provided by Jin et al (Phys. Lett. A 354 (2006) 67) F. Gao et al Phys. Lett. A 372 (2008) 3333, which is a GHZs based, entanglement and one particle transfer system, the present protocol is better secured through the data-block transfer. Further, J. Wang et al Opt. Commun. 266 (2006) 732 discloses a GHZs based system that issued one shared key for establishing user communication. The users require their mutual assistance to obtain the key. When intrusion is detected, the

communication is halt. The present protocol on the other hand is able to issue three or more keys without users assistance and controllers. The present protocol allows the communication to be carried on even when intrusion is detected.

In yet another embodiment, there is provided a QKD protocol adapted to provide communication between multiple users, wherein the producing multiple key from quantum GHZ states

While specific embodiments have been described and illustrated, it is understood that many changes, modifications, variations and combinations thereof could be made to the present invention without departing from the scope of the invention.

CLAIMS

1. A method of carrying out communication between multiple users based on a quantum key distribution (QKD), the method comprising:

generating (101) Greenberger-Horne-Zeilinger states (GHZs) by all users randomly;

distributing (102) a particle from each GHZs to form sub-sequences;

forming (103) a plurality of sequences correspond to a plurality of users based on the particles on each user, wherein one of the sequences generated by the sender comprises a home sequence;

transmitting (104) sub-sequences to the other users;

checking (105) security of the channels through verifying the sequences;

encoding (107) users' own key that are in the particles of the other users;

transmitting (108) blocks of particles and returning to the corresponding user;

retrieving (109) own initial sequences, wherein the keys of the other users are decoded;

performing (110) a GHZs measurement to obtain encoded keys by each user; and

comparing (112) the measurement results at each user site.

2. The method according to claim 1, wherein the recipient users acknowledges before establishment of the transmission.

3. The method according to claim 1, wherein the transmission (104) of the particles occurs in blocks and orders of the sequences that are not known to the recipients.

4. The method according to claim 1, wherein the GHZ triplets are n+d+d' ordered GHZ triplets.

5. The method according to claim 1, wherein the transmitting (104) sub- sequences to the users before establishing the communication.

6. The method according to claim 1, wherein the encoding (107) includes applying a unitary transformation on the particles sent by the other users.

7. The method according to claim 5, wherein the transmitting sub-sequences is carried out on the particles with the same tag number of the two different sub-sequences.

8. The method according to claim 1, wherein the checking of the security is carried out by the property of entanglement.

9. The method according to claim 1, wherein the transmission of the blocks are returning to the other partners carried out upon completion of the encoding process.

10. The method according to claim 1, wherein each of the user holds a same plurality of key as the total users.

1/1

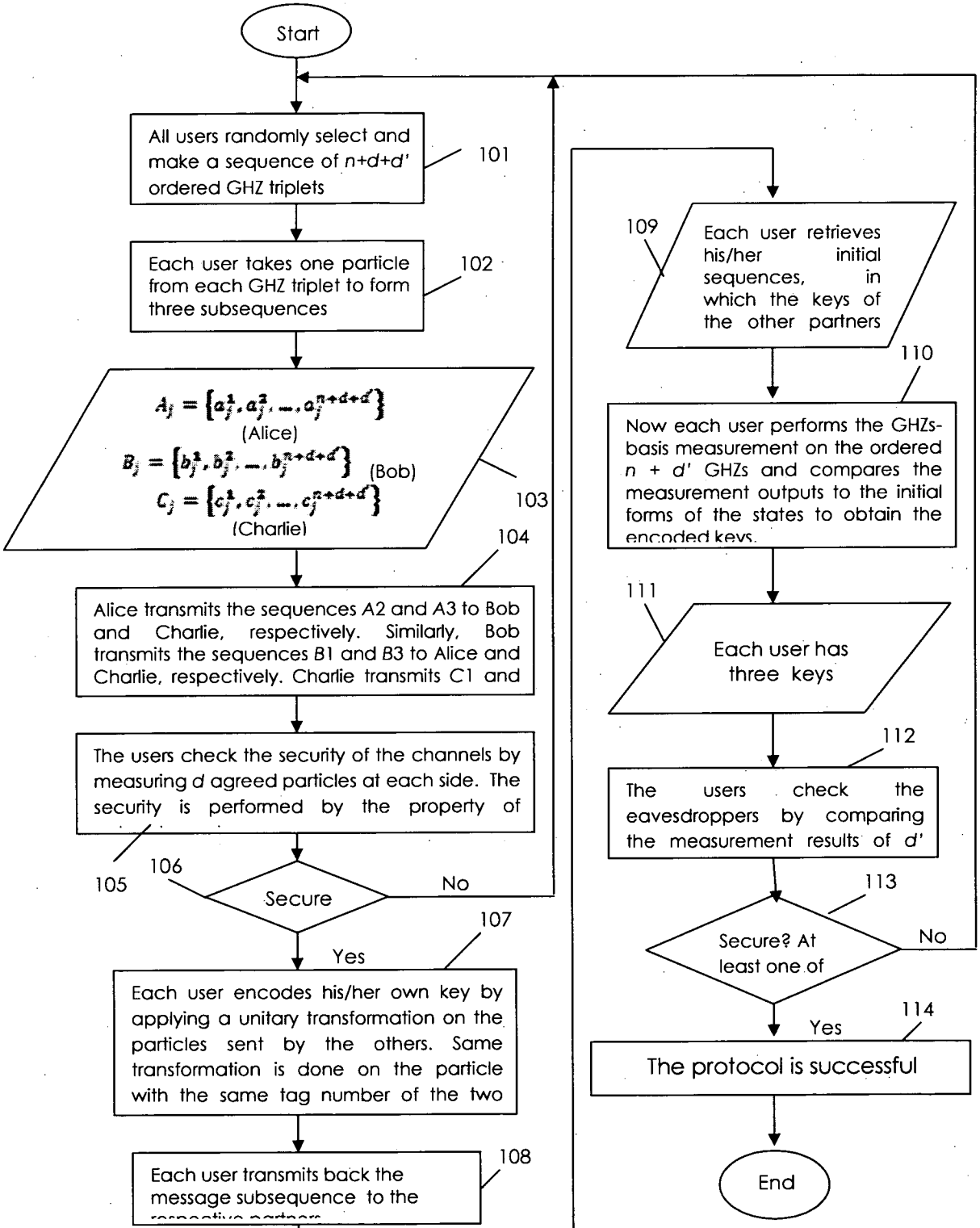
Start
All users randomly select and make a sequence of n+d+d' ordered GHZ triplets
101
Each user takes one particle from each GHZ triplet to form three subsequences
102
$A_j = \{a_j^1, a_j^2, \ldots, a_j^{n+d+d'}\}$ (Alice)
$B_j = \{b_j^1, b_j^2, \ldots, b_j^{n+d+d'}\}$ (Bob)
$C_j = \{c_j^1, c_j^2, \ldots, c_j^{n+d+d'}\}$ (Charlie)
103
Alice transmits the sequences A2 and A3 to Bob and Charlie, respectively. Similarly, Bob transmits the sequences B1 and B3 to Alice and Charlie, respectively. Charlie transmits C1 and
104
The users check the security of the channels by measuring d agreed particles at each side. The security is performed by the property of
105
106
Secure
No
Yes
107
Each user encodes his/her own key by applying a unitary transformation on the particles sent by the others. Same transformation is done on the particle with the same tag number of the two
Each user transmits back the message subsequence to the
108
109
Each user retrieves his/her initial sequences, in which the keys of the other partners
110
Now each user performs the GHZs-basis measurement on the ordered n + d' GHZs and compares the measurement outputs to the initial forms of the states to obtain the encoded keys.
111
Each user has three keys
112
The users check the eavesdroppers by comparing the measurement results of d'
113
Secure? At least one of
No
Yes
114
The protocol is successful
End

FIG. 1

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2010/000114

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

H04L 9/08 (2006.01) ***H04L 9/00*** (2006.01)

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)

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)
TXTUS0, TXTUS1, TXTUS2, TXTUS3, TXTUS4, TXTEP1, TXTGB1, TXTWO1, EPODOC, WPI, GOOGLE: Greenberger-Horne-Zeilinger, quantum, key, cryptography and similar terms.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	EL-ORANY, F. A. A. et al., 'Quantum key distribution in terms of the Greenberger-Horne-Zeilinger state: multi-key generation', version 2, 31 July 2009, pages 1 – 10, [retrieved on 23 September 2010]. Retrieved from the Internet <URL: http://arxiv.org/PS_cache/arxiv/pdf/0907/0907.4912v2.pdf>	
L, X	Pages 1 – 10.	1 – 10
A	US 2005/0249352 A1 (CHOI et al.), 10 November 2005. Whole document.	1 – 10
A	US 6678379 B1 (MAYERS et al.), 13 January 2004. Whole document.	1 – 10

☐ 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 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
7 October 2010

Date of mailing of the international search report
11 OCT 2010

Name and mailing address of the ISA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustralia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer
ANISH SINGH
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No : +61 2 6283 7915

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/MY2010/000114

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member			
US	2005249352	KR	20050100074	US	7496203
US	6678379	JP	2001007798		

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX