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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 April 2012 (26.04.2012)

PCT

(10) International Publication Number
WO 2012/053883 A1

(51) International Patent Classification:
*H04L 9/12* (2006.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/MY2010/000292

(22) International Filing Date:
25 November 2010 (25.11.2010)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 20100004904 18 October 2010 (18.10.2010) MY

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

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MOHD KHALID, Mohd Aminudin** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **AL-I@HASHIM, Norshamsuri** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **SULONG, Mohd Pazli** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **WITJAKSONO, Dr . Gunawan** [ID/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **DAMODHARAN, Ramakrishna**; Kass International Sdn. Bhd., Suite 8 - 7 -2 Menara Mutiara Bangsar, JaIan Liku Off JaIan Riong, Bangsar, 59100 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,

*[Continued on next page]*

(54) Title: SWITCHABLE INTEGRATED QUANTUM KEY DISTRIBUTION SYSTEM

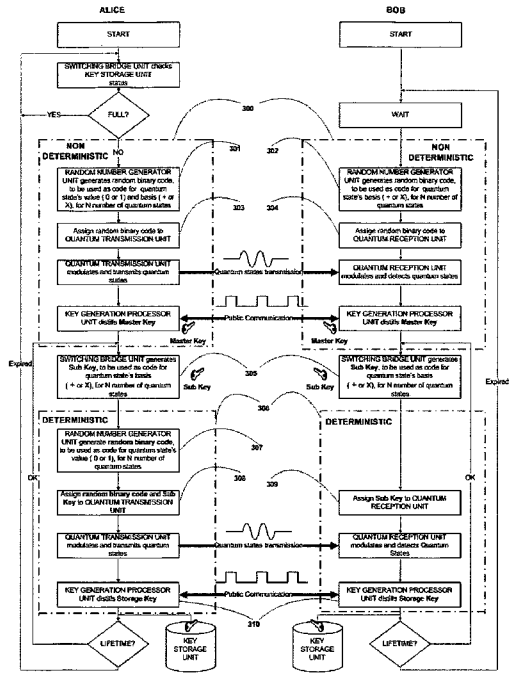


FIG 1

(57) Abstract: A switching mechanism to generate quantum key between quantum key distribution (QKD) stations using the combination of non-deterministic and deterministic QKD subsystems is disclosed. The method includes establishing a Master Key (103) using non-deterministic QKD subsystem (301 ) and buffering the Master key (103) in system memory (105). The generated Master key (103) is processed by activating Switching Bridge (305) between two protocols to generate SubKey (104). The SubKey (104) is used as preshared secret information for deterministic QKD subsystem (306). A plurality of Storage Key (105) is generated using deterministic QKD subsystem (306). The process will go back to Switching Bridge (305) to produce a new SubKey (104) when Master Key (103) is not expired. Otherwise, the Switching Bridge (305) will direct the process to non deterministic protocol to renew Master Key (103). The Storage Key (105) can be used by other application for cryptographic purposes.

WO 2012/053883 A1

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, RS, 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))*

# SWITCHABLE INTEGRATED QUANTUM KEY DISTRIBUTION SYSTEM

## FIELD OF THE INVENTION

The present invention relates generally to cryptographic systems and methods, particularly, to Quantum Key Distribution (QKD) systems and methods. More particularly, to systems and methods for integrating non-deterministic and deterministic protocols in the QKD system.

## BACKGROUND OF THE INVENTION

QKD is a method to establish secret key between QKD stations by transmitting quantum states in the form of photons. These quantum states are encoded and measured using quantum cryptographic process. The final key can be derived from quantum state detections and finally used for cryptographic purposes.

In general, QKD protocols can be divided into 2 categories: Non-deterministic protocol and deterministic. Each of these protocols has their own advantages and disadvantages.

Non-deterministic QKD protocols, such as BB84, are considered as emblematic protocols in quantum cryptography with high level of confidentiality. In BB84 protocol, an exemplary situation would be where an user, Alice randomly prepares a set of quantum states and sends it to another user, Bob. Subsequently, Bob randomly measures the quantum states. As a result, half of the quantum states will need to be discarded due to incompatible basis that are used in the measurement process. This translates to low key generation rate since many quantum states cannot be used to generate secret key.

However, deterministic protocols, such as YUEN, usually perform better than Non-deterministic protocols. However, their deterministic nature requires the system to have a pre-shared secret information. This pre-shared secret information is used by Alice to prepare quantum states and by Bob to measure the quantum states In the case of YUEN, the generated secret key will be doubled to that of BB84 since all bases are compatible,

thus a good candidate for high key availability system. However, the pre-shared secret information will need to be set before key generation process is started. The procedure to set the pre-shared secret is done manually, thus it is cumbersome and error-prone. More importantly, the level of confidentiality of deterministic protocol heavily depends on its fixed pre-shared secret information. The pre-shared secret is not changed regularly which means that any leakage of information regarding the shared secret will expose the system to cryptanalysis attack.

A high key availability system to support data encryption is essential in high data rate communication system especially when One-Time-Pad encryption is employed.

The problem in realizing QKD based One Time Pad encryption system is that it requires a large amount of encryption keys. The size of the encryption key must be equal to the size of the plaintext. Therefore, it requires a high key availability QKD system.

Non-deterministic QKD system (e.g. BB84 and SARG04) has drawbacks in term of low key generation rate. However, its security level has been proven. It offers trade-offs between high level of confidentiality and low level of key availability.

Deterministic QKD system (e.g. YUEN) has its own drawbacks as it requires pre-shared secret prior to protocol execution. This pre-shared secret can be changed but the process is manually done. The key generation rate is higher than non-deterministic protocol. It offers trade-offs between high level of key availability and low level of confidentiality and flexibility.

US2006059343 teaches a method of using final key as seed to key expansion function (e.g. stream cipher) to generate longer final key for high key availability system. This method can be applied to any type of QKD system. The disadvantage is that the expanded key is not purely derived from quantum state detections.

US5963646 teaches a solution to increase the level of secrecy of encryption key using secure deterministic method. The disadvantage of this method is that it results in shorter key.

Xiaxiang Lin et al, (An Implementation of Post-Processing Software in Quantum Key Distribution, Proceedings of 2009 World Congress on Computer Science and Information Engineering), proposes a multi-thread software architecture for high key availability QKD system. However, the proposed method focuses on post-processing stage but not at QKD protocol level which means the method still rely on the performance of optical setup.

Therefore, there exists a need for methods and systems resulting in higher key generation and higher level of secrecy.

It is an object of the invention to disclose a system that has the advantages of both deterministic and non-deterministic protocol.

It is yet another object of the invention to disclose systems and methods generating higher key generation.

It is yet another object of the invention to disclose systems and methods resulting in higher level of secrecy.

It is yet another object of the invention to disclose systems and methods that minimizes the disadvantages of non-deterministic and deterministic QKD systems to create a secure, flexible and high key availability switchable QKD system.

## SUMMARY OF THE INVENTION

The advantage of the present invention is that the disclosed methods and systems are able to achieve a balance between high key availability, high level confidentiality and system flexibility. More importantly, the generated final key is purely derived from quantum state detections.

A system to generate quantum key between QKD stations using the combination of non-deterministic and deterministic QKD system is disclosed. Also disclosed are methods, where the method includes establishing a Master Key using non-deterministic QKD system and buffering the Master key in system memory. The generated Master key is processed by activating Switching Bridge between 2 protocols to generate SubKey. The SubKey is used as preshared secret for deterministic QKD system. A plurality of Storage Key is

generated using deterministic QKD system. The process will go back to Switching Bridge to produce new SubKey when Master Key is not expired. Otherwise, the Switching Bridge will direct the process to non deterministic protocol to renew Master Key. The Storage Key can be used by other application for cryptographic purposes.

Accordingly, it is disclosed herein, a system for QKD between two stations in quantum communication state, each station comprising at least of:

a) a first subsystem (300) capable of generating a first quantum key (103);
b) a switching bridge means (305) capable of generating a SubKey (104) from the said first key; and
c) a second subsystem (306) capable of generating a second quantum key(105) using the said SubKey.

Also disclosed herein is a system for QKD between two stations in quantum communication state, each station comprising at least of a first subsystem (300) capable of generating a Master Key (103) with a life time; a switching bridge means(305) capable of generating a SubKey (104) from the said Master Key (103), a second subsystem (306) capable of generating a Storage Key(105) using the said SubKey (104) and a storage means to store the Master Key (103), SubKey (104) and Storage Key (105), wherein the said switching bridge means (305) is further capable of activating the said first subsystem (300) to generate a new Master Key (103) on the expiry of the Master Key (103).

Another aspect of the invention is a method of distributing quantum keys between two stations in quantum communication state comprising any of the steps of:

a) generating identical first quantum key (103) in a first subsystem (300) of each station by generating independently in each station a random binary code for a value of quantum state and assigning the said code for a quantum state, modulating and transmitting the said quantum state from the first station to the second station through a network and receiving the said quantum state in the second station;
b) generating a SubKey (104) in a switching bridge means using the first quantum key(103); and

c) generating a second quantum key (105) in a second subsystem (306) by using the said SubKey (104).

Yet another aspect of the invention is a method of distributing quantum keys between two stations in quantum communication state comprising any of the steps of:

a) generating identical first quantum key (103) in a first subsystem (300) of each station by generating independently in each station a random binary code for a value of quantum state and assigning the said code for a quantum state, modulating and transmitting the said quantum state from the first station to the second station through a network and receiving the said quantum state in the second station;
b) generating SubKey (104) in a switching bridge means using the first quantum key (103);
c) generating a second quantum key (105) in a second subsystem(306) by using the SubKey (104);
d) storing the first quantum key(103), SubKey (104) and second quantum key(105) in a storage device; and
e) configuring the switching bridge means (305) to check the life time of the first quantum key (103) and generate a new first quantum key (103) on the expiry of the first quantum key (103).

## BRIEF DESCRIPTION OF THE DRAWINGS

FIG 1 is a schematic representation of an embodiment of the invention.
FIG 2 is a schematic illustration of an embodiment of the invention.
FIG 3 is a schematic illustration of an embodiment of the invention.

## DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG 1, an embodiment in accordance with the principles of the invention operates firstly (100), by activating the provably secure and flexible non-deterministic QKD system to establish identical Master Key (103) between QKD stations, secondly (101), the Switching Bridge between 2 protocols is activated by generating Sub Key (104) for

subsequent step and thirdly (102), by making use of the high availability of deterministic QKD system, by using Sub Key (104) as seed to deterministic QKD system to generate Storage Key (105). The Switching Bridge is activated again when Master Key lifetime expires so that the non-deterministic QKD system can renew Master Key.

FIG 2 illustrates an exemplary implementation of the BB84/YUEN QKD system consisting of a pair of fictitious QKD stations, Alice and Bob. The internal system architecture consists of RANDOM NUMBER GENERATION UNIT (201, 205), KEY STORAGE UNIT, MEMORY BUFFER, KEY GENERATION PROCESSOR UNIT (200, 206), QUANTUM TRANSMISSION/RECEPTION UNIT (203, 207) and PUBLIC COMMUNICATION UNIT (204, 208).

RANDOM NUMBER GENERATION UNIT (201, 205) functions as source of random bit value. The random bits are used during the process of modulating/polarizing and measuring quantum state. The realization of this module can also be done with a quantum random number generator or alike.

KEY STORAGE UNIT and MEMORY BUFFER UNIT are used to store the generated cryptographic key namely, Master Key, Sub Key and Storage Key. Storage Key is stored in KEY STORAGE UNIT and other keys are stored in MEMORY BUFFER UNIT. These units can be realized by using any non-volatile memory and any volatile memory, for KEY STORAGE UNIT and MEMORY BUFFER UNIT respectively.

QUANTUM TRANSMISSION/RECEPTION UNIT (203,207) functions as transmitter and receiver to send and detect quantum states respectively. It consists of optical setup for BB84 protocol and its electronics control module such as laser driver and single photon detectors. The control logic can be implemented using microcontrollers or Field-Programmable Gate Array (FPGA). PUBLIC COMMUNICATION UNIT (204, 208) functions as network interface for public communication. This can be realized by using standard TCP/IP network interface card.

KEY GENERATION PROCESSOR UNIT (202,206) functions as main controller for the whole key generation system. It consists of SWITCHING BRIDGE UNIT (200,209), non-deterministic subsystem (ND) and deterministic subsystem (D). SWITCHING BRIDGE

UNIT manages protocol switching between BB84 and YUEN by monitoring certain conditions such as Master Key expiry and KEY STORAGE UNIT status. It is also responsible in executing error correction procedure on sifted key as well as performing privacy amplification. This unit can be realized using FPGA based embedded platform by implementing computationally intensive part such as error control coding as FPGA logic and protocol interactivity in key distillation as firmware logic on FPGA based microprocessor soft-core.

FIG 3 illustrates the detailed steps taken during the execution of switchable QKD system to generate Storage Key for cryptographic purposes. It shows the steps taken by a pair of QKD system namely, Alice and Bob.

Referring to FIG 2 and FIG 3, at Alice, SWITCHING BRIDGE UNIT (200) regularly checks KEY STORAGE UNIT, whether it is full or not. If KEY STORAGE UNIT is not full then SWITCHING BRIDGE UNIT (200) activates (300) its ND subsystem. KEY GENERATION PROCESSOR UNIT (202) at Alice informs KEY GENERATION PROCESSOR UNIT (206) at Bob through PUBLIC COMMUNICATION UNIT (204, 208) to activate Bob's ND subsystem.

At Alice (301), preparation steps prior to quantum state transmission are performed. RANDOM NUMBER GENERATION UNIT (201) at Alice generates N bits of binary code to represent basis code ("+" or "x") for N number of quantum states. Another N bits of binary code is generated to represent value code ("0" or "1") for N number of quantum states. This 2N bits of random binary code is retrieved by KEY GENERATION PROCESSOR (202) UNIT and transferred (303) to QUANTUM TRANSMISSION UNIT (203).

At Bob (302), the similar preparation steps are performed prior to quantum state transmission. RANDOM NUMBER GENERATION UNIT (205) generates N bits of binary code to represent basis code ("+" or "x") for N number of quantum states. This N bits of random binary code is transferred (304) from RANDOM NUMBER GENERATION UNIT (205) to QUANTUM RECEPTION UNIT (207) through KEY GENERATION PROCESSOR UNIT (206).

After the preparation steps have been completed, sequentially, Alice's QUANTUM TRANSMISSION UNIT (203) send quantum states by modulating or polarizing quantum signal according to its 2N bits binary code while Bob's QUANTUM RECEPTION UNIT (207) detects quantum state arrival and measure it according to its N bits binary code. The outcome of the measurement is recorded and retrieved by KEY GENERATION PROCESSOR UNIT (206) at Bob. Finally, KEY GENERATION PROCESSOR UNIT (202, 206) at Alice and Bob distill identical Master Key by performing key sifting, error correction and privacy amplification on the binary code and measurement outcome.

Subsequently, SWITCHING BRIDGE UNIT (200, 209) at Alice and Bob detects the availability of Master Key and calculates (305) current SubKey using a cryptographically strong deterministic feedback function such as secure hash function. Master Key is used as input to deterministic feedback function for the first cycle of current Master Key. For the subsequent cycle, previous SubKey is used as input to deterministic feedback function to generate current SubKey as follows:

SUBKEY[I] = F(SUBKEY[i-1]), SUBKEY[0] = Master Key

At this point, Alice and Bob share identical current SubKey which is a binary code that is used as basis code for N number of quantum states at Alice and Bob. Note that SubKey is an identical secret binary code between Alice and Bob which is derived from Master Key. This enables SWITCHING BRIDGE UNIT (200, 209) at Alice and Bob to activate (306) their D subsystem through KEY GENERATION PROCESSOR UNIT (202, 206).

Subsequently, at Alice, preparation steps prior to quantum state transmission are performed. SubKey is used to represent basis code ("+" or "x") for N number of quantum states. Another N bits of binary code is generated (307) by RANDOM GENERATOR UNIT (201) to represent value code ("0" or "1") for N number of quantum states. This 2N bits of random binary code is retrieved by KEY GENERATION PROCESSOR UNIT (202) and transferred (308) to QUANTUM TRANSMISSION UNIT (203).

At Bob, the similar preparation steps are performed prior to quantum state transmission. SubKey is used to represent basis code ("+" or "x") for N number of quantum states. This N bits of random binary code is transferred (309) from RANDOM NUMBER GENERATION

UNIT (205) to QUANTUM RECEPTION UNIT (207) through KEY GENERATION PROCESSOR UNIT (206).

After the preparation steps have been completed, sequentially, Alice's QUANTUM TRANSMISSION UNIT (203) send quantum states by modulating or polarizing quantum signal according to its 2N bits binary code while Bob's QUANTUM TRANSMISSION UNIT (203) detects quantum state arrival and measure it according to its N bits binary code. The outcome of the measurement is recorded and retrieved by KEY GENERATION PROCESSOR UNIT (206) at Bob.

Finally, KEY GENERATION PROCESSOR UNIT (202, 206) at Alice and Bob distill sifted key by performing key sifting steps on the binary code and the measurement outcome at both station. Key distillation steps heavily utilize PUBLIC COMMUNICATION UNIT (204, 208) at Alice and Bob to exchange public information. During this process, all public communication is encrypted using cryptographic algorithm such as AES or alike. Master Key is also used to perform privacy amplification on the error corrected key at Alice and Bob to produce (310) identical Storage Key. The SWITCHING BRIDGE UNIT (200, 209) continues to activate D subsystem, generate new SubKey using deterministic feedback function and use it to generate Storage Key.

The key generated by ND subsystem namely, Master Key has a lifetime. SWITCHING BRIDGE UNIT (200, 209) continuously checks whether the lifetime is expired or not. If Master Key's lifetime is expired, SWITCHING BRIDGE UNIT (200, 209) activates ND subsystem to generate new Master Key, new SubKey and finally generates Storage Key.

## CLAIMS

1. A system for Quantum Key Distribution (QKD) between two stations in quantum communication state, each station comprising at least of:
   a) a first subsystem (300) capable of generating a first quantum key(103);
   b) a switching bridge means (305) capable of generating a SubKey (104) from the said first key; and
   c) a second subsystem (306) capable of generating a second quantum key (105) using the said SubKey.

2. A system as claimed in claim 1 wherein the said first subsystem (300) further comprises of a random number generator (301) to generate random binary code for a quantum state, a quantum transmitter (303) to transmit the quantum state, a quantum receiver (304) to receive the quantum state and a key generator (310) to generate the first quantum key (103) from the received quantum state.

3. A system as claimed in claim 1 wherein the said second subsystem (306) further comprises of a random number generator (307) to generate random binary code for a quantum state, a quantum transmitter (308) to transmit the quantum state, a quantum receiver (309) to receive the quantum state and a key generator (310) to generate the second quantum key (105) from the received quantum state.

4. A system as claimed in claim 1 wherein the said first subsystem (300) is capable of generating the first quantum key (103) in accordance with a non-deterministic QKD protocol.

5. A system as claimed in claim 1 wherein the said second subsystem (300) is capable of generating the second quantum key (105) in accordance with a deterministic QKD protocol with the said SubKey (104) as the preshared secret information.

6. A system as claimed in any of the preceding claims wherein the said first quantum key (103) includes a Master Key.

7. A system as claimed in any of the preceding claims wherein the said second quantum key (105) includes a Storage Key.

8. A system for Quantum Key Distribution (QKD) between two stations in quantum communication state, each station comprising at least of a first subsystem (300) capable of generating a Master Key (103) with a life time; a switching bridge means(305) capable of generating a SubKey (104) from the said Master Key(103), a second subsystem (306) capable of generating a Storage Key(105) using the said SubKey (104) and a storage means to store the Master Key (103), SubKey (104) and Storage Key (105), wherein the said switching bridge means (305) is further capable of activating the said first subsystem (300) to generate a new Master Key (103) on the expiry of the Master Key (103).

9. A system as claimed in claim 8 wherein the said storage device includes random access memory devices or read only memory devices.

10. A method of distributing quantum keys between two stations in quantum communication state comprising any of the steps of:

a) generating identical first quantum key (103) in a first subsystem (300) of each station by generating independently in each station a random binary code for a value of quantum state and assigning the said code for a quantum state, modulating and transmitting the said quantum state from the first station to the second station through a network and receiving the said quantum state in the second station;

b) generating a SubKey (104) in a switching bridge means using the first quantum key (103); and

c) generating a second quantum key (105) in a second subsystem (306) by using the said SubKey (104).

11. A method of distributing quantum keys between two stations in quantum communication state comprising any of the steps of:

a) generating identical first quantum key (103) in a first subsystem (300) of each station by generating independently in each station a random binary code for a value of quantum state and assigning the said code for a quantum state, modulating and transmitting the said quantum state from the first station to the second station through a network and receiving the said quantum state in the second station;

b) generating SubKey (104) in a switching bridge means using the first quantum key (103);

c) generating a second quantum key (105) in a second subsystem (306) by using the SubKey (104);

d) storing the first quantum key (103), SubKey (104) and second quantum key (105) in a storage device; and

e) configuring the switching bridge means (305) to check the life time of the first quantum key (103) and generate a new first quantum key (103) on the expiry of the first quantum key (103).

12. A method as claimed in claims 10 or 11 wherein the said first subsystem (300) further comprises of a random number generator (301) to generate random binary code for a quantum state, a quantum transmitter (303) to transmit the quantum state, a quantum receiver (304) to receive the quantum state and a key generator to generate the first quantum key.

13. A method as claimed in claims 10 or 11 wherein the said second subsystem (306) further comprises of a random number generator (307) to generate random binary code for a quantum state, a quantum transmitter (308) to transmit the quantum state, a quantum receiver (309) to receive the quantum state and a key generator (310) to generate the second quantum key.

14. A method as claimed in claims 10 or 11 wherein the said first subsystem (300) is capable of generating the first quantum key (103) in accordance with a non-deterministic QKD protocol.

15. A method as claimed in claims 10 or 11 wherein the said second subsystem (300) is capable of generating the second quantum key (105) in accordance with a deterministic QKD protocol with the said SubKey (104) as the preshared secret information.

16. A method as claimed in any of the preceding claims 10-15 wherein, the said first quantum key (103) includes a Master Key.

17. A method as claimed in any of the preceding claims 10-15 wherein, the said second quantum key (105) includes a Storage Key.

18. A method as claimed in claims 10-15 wherein the said network includes a public network, a private network or open space.

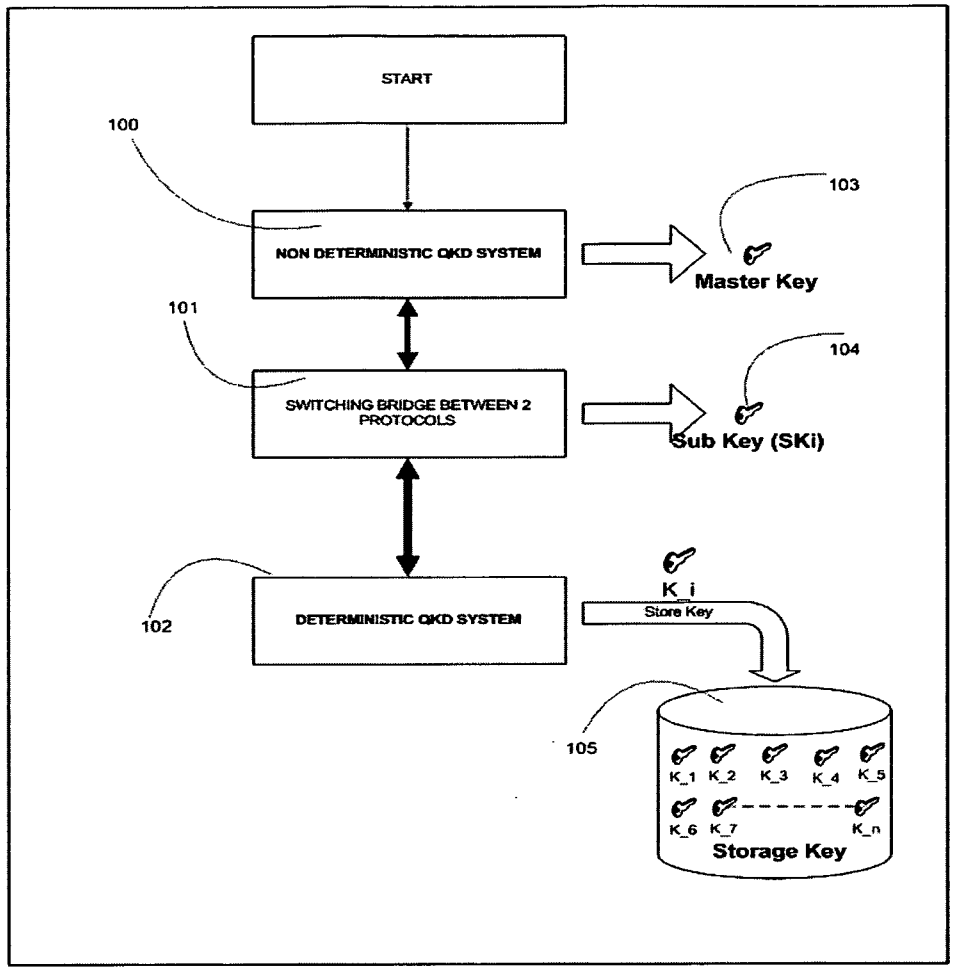
START
100
NON DETERMINISTIC QKD SYSTEM
103
Master Key
101
SWITCHING BRIDGE BETWEEN 2 PROTOCOLS
104
Sub Key (SKi)
102
DETERMINISTIC QKD SYSTEM
K_i
Store Key
105
K_1 K_2 K_3 K_4 K_5
K_6 K_7 K_n
Storage Key

FIG 1

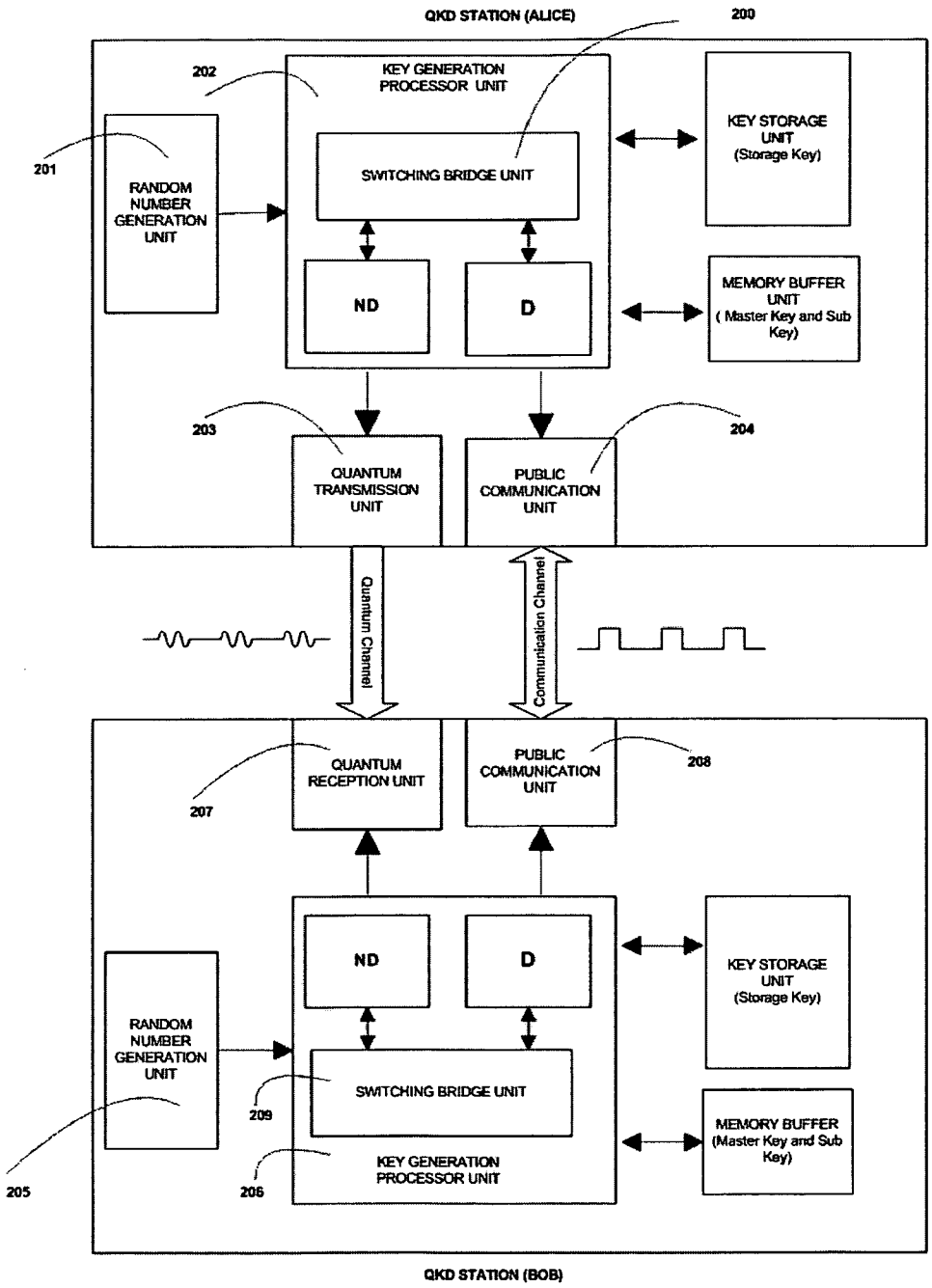
QKD STATION (ALICE)
200
202
KEY GENERATION PROCESSOR UNIT
201
RANDOM NUMBER GENERATION UNIT
SWITCHING BRIDGE UNIT
KEY STORAGE UNIT (Storage Key)
ND
D
MEMORY BUFFER UNIT ( Master Key and Sub Key)
203
204
QUANTUM TRANSMISSION UNIT
PUBLIC COMMUNICATION UNIT
Quantum Channel
Communication Channel
QUANTUM RECEPTION UNIT
207
PUBLIC COMMUNICATION UNIT
208
ND
D
KEY STORAGE UNIT (Storage Key)
RANDOM NUMBER GENERATION UNIT
SWITCHING BRIDGE UNIT
209
MEMORY BUFFER (Master Key and Sub Key)
205
206
KEY GENERATION PROCESSOR UNIT
QKD STATION (BOB)

FIG 2

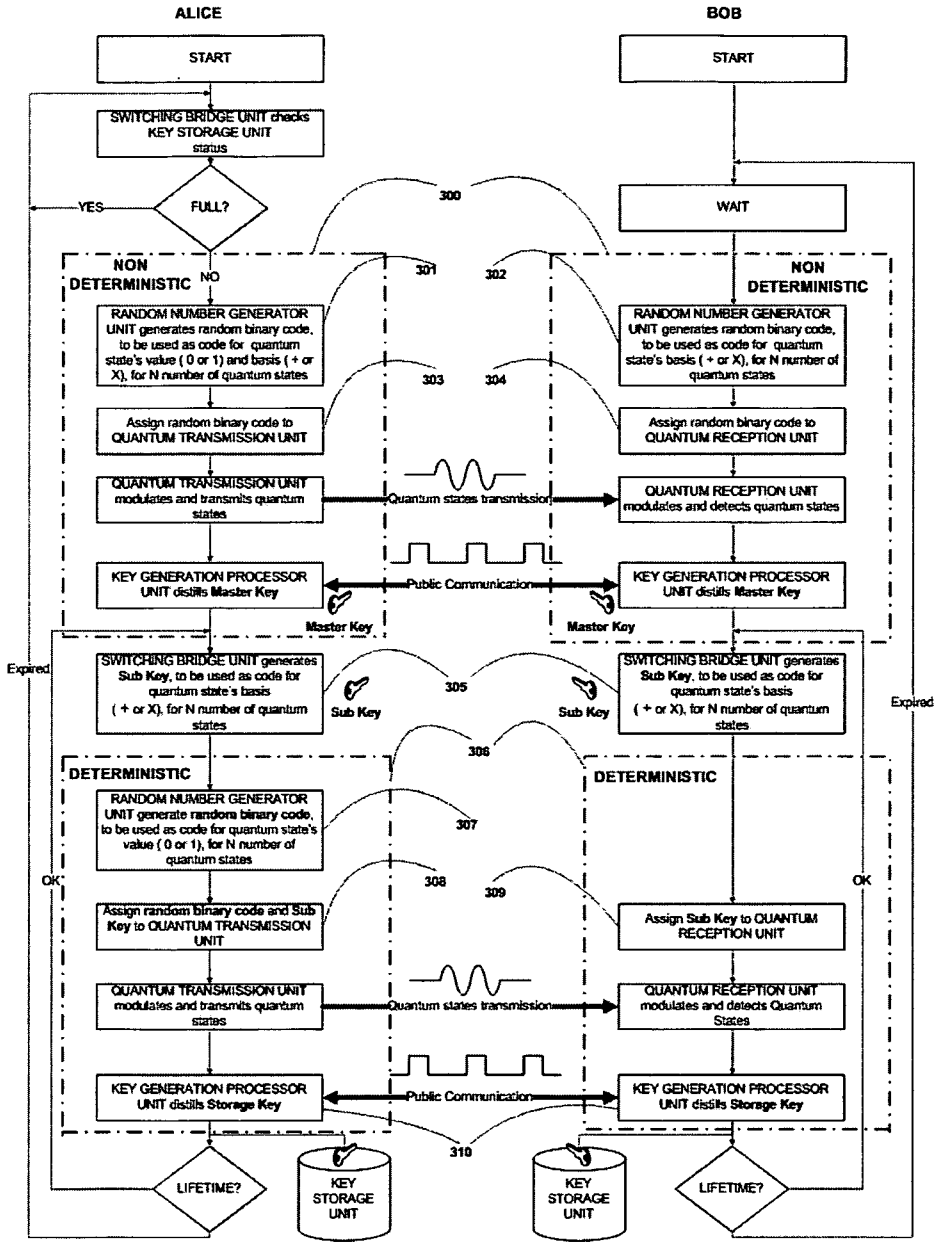
ALICE
BOB
START
START
SWITCHING BRIDGE UNIT checks KEY STORAGE UNIT status
FULL?
YES
NO
300
WAIT
NON DETERMINISTIC
NON DETERMINISTIC
301
302
RANDOM NUMBER GENERATOR UNIT generates random binary code, to be used as code for quantum state's value ( 0 or 1) and basis ( + or X), for N number of quantum states
RANDOM NUMBER GENERATOR UNIT generates random binary code, to be used as code for quantum state's basis ( + or X), for N number of quantum states
303
304
Assign random binary code to QUANTUM TRANSMISSION UNIT
Assign random binary code to QUANTUM RECEPTION UNIT
QUANTUM TRANSMISSION UNIT modulates and transmits quantum states
Quantum states transmission
QUANTUM RECEPTION UNIT modulates and detects quantum states
KEY GENERATION PROCESSOR UNIT distills Master Key
Public Communication
KEY GENERATION PROCESSOR UNIT distills Master Key
Master Key
Master Key
Expired
SWITCHING BRIDGE UNIT generates Sub Key, to be used as code for quantum state's basis ( + or X), for N number of quantum states
305
Sub Key
Sub Key
SWITCHING BRIDGE UNIT generates Sub Key, to be used as code for quantum state's basis ( + or X), for N number of quantum states
Expired
306
DETERMINISTIC
DETERMINISTIC
RANDOM NUMBER GENERATOR UNIT generate random binary code, to be used as code for quantum state's value ( 0 or 1), for N number of quantum states
307
OK
308
309
OK
Assign random binary code and Sub Key to QUANTUM TRANSMISSION UNIT
Assign Sub Key to QUANTUM RECEPTION UNIT
QUANTUM TRANSMISSION UNIT modulates and transmits quantum states
Quantum states transmission
QUANTUM RECEPTION UNIT modulates and detects Quantum States
KEY GENERATION PROCESSOR UNIT distills Storage Key
Public Communication
KEY GENERATION PROCESSOR UNIT distills Storage Key
310
LIFETIME?
KEY STORAGE UNIT
KEY STORAGE UNIT
LIFETIME?

FIG 1

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/MY2010/000292**

**A. CLASSIFICATION OF SUBJECT MATTER**

***H04L 9/12(2006.01)i, H04L 9/08(2006.01)i***

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)

H04L 9/12; H04L 9/08; H04K 1/00; H03M 13/00; H04L 9/00

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: quantum key, distribution, master key, subkey, storage key and random.

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| A | US 2008-0101612 A1 (IMAI HIDEKI et al.) 01 May 2008<br>See abstract, paragraphs [45],[52]-[55],[68]-[73], figures 1,2,7 and claims 1,2,8. | 1-18 |
| A | US 2006-0059403 A1 (YOUDAI WATANABE) 16 March 2006<br>See abstract, paragraphs [63]-[65],[69]-[70], figures 1,2A,2B and claim 1. | 1-18 |
| A | US 2007-0014415 A1 (KEITH HARRISON et al.) 18 January 2007<br>See abstract, paragraphs [54]-[60],[65]-[67], figures 2-4B and claims 1-5. | 1-18 |

☐ 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 citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 25 OCTOBER 2011 (25.10.2011) | **25 OCTOBER 2011 (25.10.2011)** |


Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Cheongsa-ro,
Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Yang, Jong Phil

Telephone No. 82-42-481-8595

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/MY2010/000292**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2008-0101612 A1 | 01.05.2008 | GB 2433399 A | 20.06.2007 |
| | | JP 04-555979 B2 | 30.07.2010 |
| | | JP W020-060254 10A1 | 09.03.2006 |
| | | US 7936883 B2 | 03.05.2011 |
| | | WO 2006-025410 A1 | 09.03.2006 |
| US 2006-0059403 A1 | 16.03.2006 | AU 2003-262096 A1 | 08.04.2004 |
| | | CA 2499357 A1 | 01.04.2004 |
| | | CN 1706147 A | 07.12.2005 |
| | | CN 1706147 C0 | 07.12.2005 |
| | | EP 1542390 A1 | 15.06.2005 |
| | | EP 1542390 A4 | 17.11.2010 |
| | | JP 04-290401 B2 | 10.04.2009 |
| | | JP 2004-112278 A | 08.04.2004 |
| | | KR 10-0697476 B1 | 20.03.2007 |
| | | KR 10-2006-0059853 A | 02.06.2006 |
| | | NO 20042553 A | 21.12.2004 |
| | | US 7609839 B2 | 27.10.2009 |
| | | WO 2004-028074 A1 | 01.04.2004 |
| US 2007-0014415 A1 | 18.01.2007 | GB 0512229 D0 | 27.07.2005 |
| | | GB 0611946 D0 | 26.07.2006 |
| | | GB 2427337 A | 20.12.2006 |
| | | GB 2427337 B | 20.01.2010 |
| | | GB 2430775 A | 04.04.2007 |
| | | GB 2430845 A | 04.04.2007 |
| | | GB 2430846 A | 04.04.2007 |
| | | GB 2430847 A | 04.04.2007 |
| | | GB 2430848 A | 04.04.2007 |
| | | GB 2430850 A | 04.04.2007 |
| | | US 2007-0016534 A1 | 18.01.2007 |
| | | US 2007-0016794 A1 | 18.01.2007 |
| | | US 2007-0025551 A1 | 01.02.2007 |
| | | US 2007-0074276 A1 | 29.03.2007 |
| | | US 2007-0074277 A1 | 29.03.2007 |
| | | US 2007-0101410 A1 | 03.05.2007 |
| | | US 2007-0172054 A1 | 26.07.2007 |
| | | US 2007-0177424 A1 | 02.08.2007 |
| | | US 7721955 B2 | 25.05.2010 |
| | | US 7864958 B2 | 04.01.2011 |