

QUANTUM KEY DISTRIBUTION METHOD, APPARATUS AND SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to Chinese Patent Application No.
5 202310341896.9, entitled “METHOD, APPARATUS AND SYSTEM FOR
QUANTUM KEY DISTRIBUTION” and filed with the Chinese Patent
Office on March 31, 2023, the entire content of which is incorporated herein
by reference.

TECHNICAL FIELD

10 The present invention relates to the field of quantum communication,
and in particular to a method, an apparatus and a system for quantum key
distribution.

BACKGROUND

Quantum key distribution (QKD) technology is developed to ensure
15 the security of communication by virtue of the properties of quantum
mechanics, whereby both communicating parties can generate and share a
random and secure key to encrypt and decrypt messages. It has a wide
application range in fields such as practical cryptography, information
security and national defense, as well as in various secure communication
20 environments.

A major challenge for QKD systems is how to realize more practical,

stable, and low-cost implementations based on optical devices. In most existing systems, for security reasons, the signal intensity is controlled at the single-photon level. Together with channel attenuation (e.g., optical fiber), the receiver typically employs high-sensitivity single-photon detectors (SPDs). Such detectors are costly and prone to issues such as dark counts and dead time, which lower detection efficiency and increase error rates.

Hence, there is a need for a new QKD scheme.

SUMMARY OF THE INVENTION

Embodiments of the present invention provide a method, an apparatus and a system for quantum key distribution (QKD). The method allows the receiver in QKD to measure signal light using a coherent detection detector rather than an expensive high-sensitivity SPD. Consequently, the measurement equipment is lower-cost and effectively avoids the efficiency loss and error problems caused by dark counts and dead time inherent to SPDs.

To solve the above technical problem, the present invention employs the following technical solutions. In a first aspect, there is provided a method for quantum key distribution in which participants include a first party and a second party, the method comprising:

the first party preparing a coherent pulse having a first optical intensity and a first phase, and transmitting the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a

first key bit included in an original key of the first party;

the second party receiving the coherent pulse and preparing a local oscillator pulse having a second optical intensity and a second phase, and inputting the coherent pulse and the local oscillator pulse into a coherent
 5 detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

the second party comparing the measurement result with a first threshold agreed upon by the first party and the second party; if the
 10 measurement result satisfies a preset relation with the first threshold, determining a second key bit corresponding to the first key bit at the second party, and releasing the second random value to the first party; and

the first party determining whether to flip the first key bit based on the first random value and the second random value.

15 Preferably, the method further comprises:

if the measurement result does not satisfy the preset relation with the first threshold, abandoning the determination of the second key bit corresponding to the first key bit at the second party.

Preferably, the first optical intensity is randomly selected from multiple
 20 preset intensity values.

Preferably, the first phase is expressed as:

$$\phi_i = \phi_i^a + \pi\kappa_a^i$$

where ϕ_i denotes the first phase, ϕ_i^a denotes the first random value, and κ_a^i denotes the first key bit.

Preferably, the first random value is randomly selected by the first party from $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D - 1$; D is a natural number), and the second random
 5 value is randomly selected by the second party from $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D - 1$; D is a natural number).

Preferably, the first threshold is greater than 0; and the step of if the measurement result satisfies a preset relation with the first threshold, determining a second key bit corresponding to the first key bit at the second
 10 party comprises: if the measurement result is greater than the first threshold, determining the second key bit to be 0.

Preferably, the first threshold is greater than 0; and the step of if the measurement result satisfies a preset relation with the first threshold, determining a second key bit corresponding to the first key bit at the second
 15 party comprises: if the measurement result is less than the negative of the first threshold, determining the second key bit to be 1.

Preferably, the step of the first party determining whether to flip the first key bit based on the first random value and the second random value comprises: if the absolute value of the difference between the first random
 20 value and the second random value falls within a preset range, flipping the first key bit.

In a second aspect, there is provided a method for quantum key distribution in which participants include a first party and a second party, the method being executed by the first party, comprising:

5 preparing a coherent pulse having a first optical intensity and a first phase, and transmitting the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

obtaining a second random value released by the second party; and

10 determining whether to flip the first key bit based on the first random value and the second random value.

In a third aspect, there is provided a method for quantum key distribution in which participants include a first party and a second party, the method being executed by the second party, comprising:

15 receiving a coherent pulse from the first party, and preparing a local oscillator pulse having a second optical intensity and a second phase, wherein the second optical intensity is greater than the first optical intensity of the coherent pulse, and the second phase is determined according to a second random value; inputting the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result; and

20 comparing the measurement result with a first threshold; if the measurement result satisfies a preset relation with the first threshold, determining a second key bit and releasing the second random value to the first party, wherein the first threshold is agreed upon by the first party and

the second party.

In a fourth aspect, there is provided a system for quantum key distribution comprising a first party and a second party as participants, wherein:

5 the first party is configured to prepare a coherent pulse having a first optical intensity and a first phase, and to transmit the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

10 the second party is configured to receive the coherent pulse and prepare a local oscillator pulse having a second optical intensity and a second phase, and to input the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

15 the second party is further configured to compare the measurement result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, to determine a second key bit corresponding to the first key bit at the second party and to release the second random value to the first party;

20 and

 the first party is further configured to determine whether to flip the first key bit based on the first random value and the second random value.

In a fifth aspect, there is provided an apparatus for quantum key distribution in which participants include a first party and a second party, the apparatus being disposed at the first party, comprising:

5 a preparation unit configured to prepare a coherent pulse having a first optical intensity and a first phase, and to transmit the coherent pulse to a second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

an obtention unit configured to obtain a second random value released by the second party; and

10 a determination unit configured to determine whether to flip the first key bit based on the first random value and the second random value.

In a sixth aspect, there is provided an apparatus for quantum key distribution in which participants include a first party and a second party, the apparatus being disposed at the second party, comprising:

15 a measurement unit configured to receive a coherent pulse from the first party, to prepare a local oscillator pulse having a second optical intensity and a second phase, wherein the second optical intensity is greater than the first optical intensity of the coherent pulse, and the second phase is determined according to a second random value; and to input the coherent pulse and the
20 local oscillator pulse into a coherent detection module to obtain a measurement result; and

a determination unit configured to compare the measurement result with a first threshold; if the measurement result satisfies a preset relation with the

first threshold, to determine a second key bit and release the second random value to the first party, wherein the first threshold is agreed upon by the first party and the second party.

5 BRIEF DESCRIPTION OF THE DRAWINGS

To describe the technical solutions in the embodiments of the present invention more clearly, the following briefly introduces the accompanying drawings required for describing the embodiments. Obviously, the accompanying drawings in the following description show merely some
10 embodiments of the present invention, and a person of ordinary skills in the art may still derive other drawings from these accompanying drawings without creative efforts.

FIG. 1 is a schematic diagram of a scheme using a single-photon detector in quantum key distribution;

15 FIG. 2A is a schematic diagram of a quantum key distribution scheme according to an embodiment of the present invention;

FIG. 2B is a structural schematic diagram of a coherent detection module according to an embodiment of the present invention;

FIG. 3 is a flowchart of a method for quantum key distribution according
20 to an embodiment of the present invention;

FIG. 4 is a flowchart of a method for quantum key distribution according to another embodiment of the present invention;

FIG. 5 is a flowchart of a method for quantum key distribution according

to still another embodiment of the present invention;

FIG. 6 is a structural diagram of a system for quantum key distribution according to an embodiment of the present invention;

FIG. 7 is a structural diagram of an apparatus for quantum key
5 distribution according to an embodiment of the present invention;

FIG. 8 is a structural diagram of an apparatus for quantum key distribution according to another embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

10 To make the objectives, technical solutions, and advantages of the embodiments of the present invention clear, the embodiments of the present invention will be described in detail below with reference to the accompanying drawings. It should be understood that the embodiments described herein are merely illustrative and are not intended to limit all
15 possible embodiments of the present invention. Based on the embodiments in the description, all other embodiments that may be conceived by those skilled in the art without inventive effort shall fall within the scope of protection of the present invention.

As described above, in most existing quantum key distribution (QKD)
20 systems, for security considerations, the intensity of the transmitted light signal is controlled at the single-photon level. Furthermore, with the attenuation of the transmission channel such as an optical fiber, the signal

intensity received at the measurement side is often very weak. Therefore, the measurement side usually employs a highly sensitive single-photon detector to measure the received signal. FIG. 1 is a schematic diagram of a scheme using a single-photon detector in quantum key distribution. As shown in FIG. 5 1, the transmitting end (e.g., Alice end) may generate a light signal at the single-photon level by means of a light source and encode key information into the light signal. The light signal is then transmitted through a transmission channel (e.g., an optical fiber) to a receiving end. The receiving end (e.g., Bob end) , after receiving the light signal, may perform optical 10 preprocessing on the signal (e.g., beam splitting) , then measure the light signal with a single-photon detector, and determine the key information based on the measurement result.

However, this scheme suffers from the following problems. On the one hand, single-photon detectors are often very expensive, which results in high 15 costs for key distribution. On the other hand, the use of single-photon detectors may also lead to lower detection efficiency and higher detection error rates due to issues such as dark counts and dead time. The term “dark count” refers to the phenomenon that, due to the high sensitivity of the single-photon detector, stray light (non-signal light) and electrical noise are likely 20 to be mistakenly regarded by the detector as valid signal photons; such misjudgment is referred to as a dark count. The term “dead time” refers to the fixed period of time (e.g., 20 ns) that a single-photon detector typically requires to fully discharge the capacitor after detecting a photon before it

can detect the next photon. Because photons cannot be detected during the dead time, omissions in measurement data may occur.

To address the above issues, embodiments of the present specification provide a new quantum key distribution (QKD) scheme. FIG. 2A is a schematic diagram of a quantum key distribution scheme according to an embodiment of the present invention. As shown in Figure 2A, transmitting end (Alice end) generates a coherent optical signal using a coherent light source and encodes the key information into this coherent optical signal. The signal is then transmitted to the receiver through the transmission channel.

5 The receiving end (e.g., Bob end) receives the coherent optical signal and prepares a corresponding local oscillator pulse. After optional optical preprocessing of the signal, the coherent pulse and the local oscillator pulse are input into a coherent detection module to obtain the measurement results.

10 The key information is then determined based on these measurement results.

15 FIG. 2B is a structural schematic diagram of a coherent detection module according to an embodiment of the present invention. As illustrated, the incoming signal light and the local oscillator light respectively enter a beam splitter, where they interfere with each other, and are then directed to two detectors. After obtaining classical measurement results, the detectors

20 send the results to a post-processing module, which performs a certain computation—typically subtraction—to obtain the final measurement result.

It should be emphasized that the detectors used here do not need to be highly

sensitive single-photon detectors; ordinary detectors suffice.

The advantages of the QKD scheme presented above are that, by encoding and extracting key information based on coherent light, and by replacing single-photon detectors with a coherent detection module, the error
5 rate of measurement results can be reduced. Furthermore, the coherent detection module can employ ordinary detectors that are significantly more cost-effective, thereby reducing the overall expense of quantum key distribution.

The QKD scheme provided by the embodiments of the present
10 specification is described in detail below. FIG. 3 is a flowchart of a method for quantum key distribution according to an embodiment of the present invention. The participants in the QKD process include a first party and a second party. As shown in FIG. 3, the method at least comprises the following steps:

15 step 31, the first party preparing a coherent pulse having a first optical intensity and a first phase, and transmitting the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

step 32, the second party receiving the coherent pulse and preparing a
20 local oscillator pulse having a second optical intensity and a second phase, and inputting the coherent pulse and the local oscillator pulse into a coherent

detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

step 33, the second party comparing the measurement result with a first
5 threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, determining a second key bit corresponding to the first key bit at the second party, and releasing the second random value to the first party; and

step 34, the first party determining whether to flip the first key bit based
10 on the first random value and the second random value.

First, in step 31, the first party prepares a coherent pulse having a first optical intensity and a first phase, and transmits the coherent pulse to the second party.

In one embodiment, the first party may generate coherent-state pulse
15 using a quantum coherent light source. Through intensity and phase modulation, the first party obtains coherent pulse having a first optical intensity and a first phase, and then transmits the modulated coherent pulse to the second party via a transmission channel.

In different embodiments, the value of the first optical intensity may
20 vary. In one embodiment, the first optical intensity may be randomly selected from multiple preset intensity values. In a specific embodiment, for example,

the first optical intensity may be randomly selected from among the three values $0, \nu, \mu$ (where $0 < \nu < \mu$).

The first phase may be determined according to a first random value and a first key bit included in an original key of the first party. In different
5 embodiments, the manner of determining the first phase may vary. In one embodiment, the first phase may be expressed as:

$$\phi_i = \phi_i^a + \pi \kappa_a^i$$

where ϕ_i denotes the first phase, ϕ_i^a denotes the first random value, and $\kappa_a^i \in \{0,1\}$ denotes the first key bit, which is one bit from the original
10 key held by the first party and to be distributed.

In a specific embodiment, the first random value ϕ_i^a may be randomly determined by the first party from $\frac{2\pi}{D}k$, where $k=0,1,\dots,D-1$; and D is a natural number.

In one embodiment, prior to step 31, the first party and the second party
15 may calibrate the communication clock and initial phase of the channel, as well as perform mutual authentication of their identities.

Each participant may execute its corresponding steps through its terminal. The term “terminal” here does not exclusively refer to a single workstation device of a participant; rather, it may be any computing device
20 used by the participant for computational processing, including but not limited to servers, workstations, minicomputers, or mobile processing

terminals. It may also comprise coordinated operation of multiple computing devices of a participant. Since the QKD process can include both quantum operations and post-processing, in some embodiments, a participant's terminal may also include a quantum-classical hybrid server. The hybrid
5 server comprises both a quantum processor and a classical processor, where the quantum processor executes the quantum operation portion, and the classical processor executes the post-processing portion.

Then, in step 32, the second party receives the coherent pulse and prepares a local oscillator pulse having a second optical intensity and a
10 second phase, and inputs the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result. The second phase is determined according to a second random value.

In this step, the second party may, for example, determine a second phase based on a second random value, and prepare local oscillator light with
15 the corresponding phase and a second optical intensity using a local oscillator light source. The received signal light and the prepared local oscillator light are then input into a coherent measurement module for measurement, thereby obtaining a measurement result.

Theoretically, the second optical intensity can be much greater than the
20 first optical intensity. Therefore, in one embodiment, the second optical intensity may be greater than the first optical intensity. In another embodiment, the second optical intensity may exceed the first optical

intensity by a preset multiple. In different specific embodiments, the preset multiple may take different specific values.

The second phase may be determined based on the second random value. In one embodiment, the second random value ϕ_i^b may be randomly selected
 5 by the second party from $\frac{2\pi}{D}k$ ($k = 0, 1, \dots, D - 1$; D is a natural number).

Based on the above-prepared local oscillator light, the second party inputs the received coherent pulse together with the prepared local oscillator pulse into a coherent detection module. Referring to Figure 2B, the received coherent pulse and the local oscillator pulse interfere with each other through
 10 a beam splitter and are then directed into two detectors. Each detector outputs a classical measurement result, which are then processed by a post-processing module. For example, a subtraction operation is performed on the two classical measurement results, and the result of this operation is taken as the measurement result n_i .

15 Next, in step 33, the second party compares the measurement result with a first threshold agreed upon or preset by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, determines a second key bit at the second party corresponding to the first key bit, and releases the second random value to the first party.

20 In this step, if the measurement result n_i satisfies a preset relationship with a first threshold value n_{th} , it is indicated that the correctness of

transmitting the first key bit is relatively high. Therefore, the corresponding key bit at the second party (i.e., the second key bit, representing the bit received by the second party) can be determined. Specifically, in different embodiments, the value of the first threshold n_{th} and the preset relationship may vary. In one embodiment, for example, the first threshold n_{th} may be greater than 0. If the measurement result is greater than the threshold, i.e., $n_i > n_{th}$, then the second key bit is determined to be 0. In another embodiment, if the measurement result is less than the negative of the threshold, i.e., $n_i < -n_{th}$, then the second key bit is determined to be 1.

If the measurement result n_i does not satisfy the preset relationship with the first threshold n_{th} , it is indicated that the correctness of transmitting the first key bit is relatively low. Therefore, the corresponding key bit at the second party (the second key bit) may be discarded. In one embodiment, if the measurement result does not satisfy the preset relation with the first threshold, the determination of the second key bit corresponding to the first key bit at the second party is abandoned.

After the second party determines the second key bit, it may release the second random value to the first party. Since the original key of the first party may include multiple key bits, steps 31–33 may be executed for multiple rounds (corresponding to multiple key bits). Therefore, in one embodiment, after multiple rounds are executed, the second party may release to the first party the rounds in which the corresponding key bits were not discarded,

together with the second random values corresponding to those rounds.

Then, in step 34, the first party determines whether to flip the first key bit, based on the first random value and the second random value.

In practical scenarios, if the difference between the first random value
 5 selected by the first party and the second random value selected by the second
 party falls within a specific range, the second key bit determined by the
 second party is often not the original value of the first key bit, but rather its
 flipped value (e.g., 0 becomes 1, and 1 becomes 0). Therefore, after obtaining
 the second random value released by the second party, the first party can
 10 check whether the difference between the two random values lies within the
 specific range. Based on the comparison result, the first party can decide
 whether to flip its own original first key bit in order to remain consistent with
 the second key bit determined by the second party.

In one embodiment, if the absolute value of the difference between the
 15 first random value and the second random value falls within a preset range,
 then the first key bit is flipped (i.e., 0 becomes 1, and 1 becomes 0). In
 different embodiments, the preset range may vary. In a specific embodiment,
 the preset range may be $[\frac{1}{2}\pi, \frac{3}{2}\pi)$. That is, if $|\phi_i^a - \phi_i^b| \in [\frac{1}{2}\pi, \frac{3}{2}\pi)$, then the
 first key bit is flipped; otherwise, the first key bit is not flipped.

20 As mentioned above, steps 31–33 may be executed for multiple rounds
 (corresponding to multiple key bits). Therefore, in one embodiment, the first

party may, for the rounds in which the second party has not discarded the confirmation of its corresponding key bits and for which the second random values are released, determine whether to flip its own first key bits in those rounds. Consequently, the first party and the second party can determine their
5 retained keys based on the key bits respectively determined in all non-discarded rounds.

To further improve the accuracy of the retained keys of both parties and to enhance the security of key distribution, in one embodiment, the first party and the second party may also perform information reconciliation and/or
10 privacy amplification based on their respective keys. Information reconciliation is mainly used to ensure that the keys held by all users are identical, i.e., to guarantee key consistency. Privacy amplification is mainly used to ensure that potential eavesdroppers cannot obtain useful information about the keys, thereby guaranteeing key security. In different specific
15 embodiments, the specific ways in which the first party and the second party perform information reconciliation and/or privacy amplification may vary, and the present specification imposes no limitation thereon.

In summary, the method for quantum key distribution provided by the embodiments of the present invention enables information encoding, optical
20 signal transmission, and key extraction based on coherent light, while replacing the single-photon detector with a coherent detection module. On the one hand, this scheme significantly reduces the error rate in optical signal

measurement and improves measurement efficiency. On the other hand, compared with conventional schemes that rely on costly single-photon detectors, the present method allows the use of inexpensive ordinary photodetectors for optical signal measurement, thereby also significantly
5 reducing the cost of quantum key distribution.

FIG. 4 is a flowchart of a method for quantum key distribution according to another embodiment of the present invention. The participants of the QKD include a first party and a second party, the method being executed by the first party. As shown in FIG. 4, the method at least comprises the following
10 steps:

step 41, preparing a coherent pulse having a first optical intensity and a first phase, and transmitting the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

15 step 42, obtaining a second random value released by the second party upon determining that a measurement result satisfies a preset relation with a first threshold, the measurement result being obtained by the second party by inputting a local oscillator pulse having a second optical intensity and a second phase and the coherent pulse into a coherent detection module,
20 wherein the second optical intensity is greater than the first optical intensity and the second phase is determined according to the second random value; the first threshold being agreed upon by the first party and the second party;

and

step 43, determining whether to flip the first key bit based on the first random value and the second random value.

FIG. 5 is a flowchart of a method for quantum key distribution according to still another embodiment of the present invention. The participants of the QKD include a first party and a second party, the method being executed by the second party. As shown in FIG. 5, the method at least comprises the following steps:

step 51, receiving a coherent pulse having a first optical intensity and a first phase from the first party, wherein the first phase is determined according to a first random value held by the first party and a first key bit included in an original key of the first party; preparing a local oscillator pulse having a second optical intensity and a second phase, wherein the second optical intensity is greater than the first optical intensity of the coherent pulse, and the second phase is determined according to a second random value; inputting the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result; and

step 52, comparing the measurement result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, determining a second key bit corresponding to the first key bit at the second party and releasing the

second random value to the first party to make the first party to determine whether to flip the first key bit based on the first random value and the second random value.

According to yet another aspect of the embodiments, a system for QKD
5 is also provided. FIG. 6 is a structural diagram of a system for quantum key distribution according to an embodiment of the present invention. As shown in FIG. 6, the system comprising a first party 61 and a second party 62 as participants, wherein:

the first party 61 is configured to prepare a coherent pulse having a first
10 optical intensity and a first phase, and to transmit the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

the second party 62 is configured to receive the coherent pulse and
prepare a local oscillator pulse having a second optical intensity and a second
15 phase, and to input the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

the second party 62 is further configured to compare the measurement
20 result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first

threshold, to determine a second key bit corresponding to the first key bit at the second party and to release the second random value to the first party; and

the first party 61 is further configured to determine whether to flip the first key bit based on the first random value and the second random value.

According to yet another aspect of the embodiments, a system for QKD is also provided. FIG. 7 is a structural diagram of a system for quantum key distribution according to an embodiment of the present invention. As shown in FIG. 6, the system comprising a first party 610 and a second party 620 as participants, wherein:

the first party 610 is configured to prepare a coherent pulse having a first optical intensity and a first phase, and to transmit the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

the second party 620 is configured to receive the coherent pulse and prepare a local oscillator pulse having a second optical intensity and a second phase, and to input the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

the second party 620 is further configured to compare the measurement

result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, to determine a second key bit corresponding to the first key bit at the second party and to release the second random value to the first party;

5 and

the first party 610 is further configured to determine whether to flip the first key bit based on the first random value and the second random value.

In one embodiment, the first party 610 may include an apparatus for quantum key distribution. As shown in FIG. 7, the apparatus comprises:

10 a preparation unit 611 configured to prepare a coherent pulse having a first optical intensity and a first phase, and to transmit the coherent pulse to a second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

an obtention unit 612 configured to obtain a second random value
15 released by the second party upon determining that a measurement result satisfies a preset relation with a first threshold, the measurement result being obtained by the second party by inputting a local oscillator pulse having a second optical intensity and a second phase and the coherent pulse into a coherent detection module, wherein the second optical intensity is greater
20 than the first optical intensity and the second phase is determined according to the second random value; the first threshold being agreed upon by the first

party and the second party; and

a determination unit 613 configured to determine whether to flip the first key bit based on the first random value and the second random value.

In one embodiment, the second party 620 may include an apparatus for
5 quantum key distribution. As shown in FIG. 8, the apparatus comprises:

a measurement unit 621 configured to receive a coherent pulse having a first optical intensity and a first phase from the first party, wherein the first phase is determined according to a first random value held by the first party and a first key bit included in an original key of the first party; to prepare a
10 local oscillator pulse having a second optical intensity and a second phase, wherein the second optical intensity is greater than the first optical intensity of the coherent pulse, and the second phase is determined according to a second random value; and to input the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result; and

15 a determination unit 622 configured to compare the measurement result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, to determine a second key bit corresponding to the first key bit at the second party and release the second random value to the first party to enable the first
20 party to determine whether to flip its first key bit based on the first random value and the second random value.

According to an embodiment in a further another aspect, a computer-readable medium storing a computer program is further provided. The computer program, when running, executes the method described above.

According to an embodiment in a further another aspect, a computing
5 device is further provided. The computing device includes a memory and a processor; the memory stores executable codes; and the processor, when executing the executable codes, implements the method described above.

The specific embodiments of the present invention are described above. Other embodiments shall fall within the scope of the appended claims. In
10 some cases, the operations and steps stated in the claims can be executed in an order different from that in the embodiments to achieve a desired result as well. In addition, the processes depicted in the accompanying drawings are not necessarily performed based on the illustrated specific order or continuous order to achieve the desired result. In some embodiments, multi-
15 task processing and parallel processing are also possible or may be advantageous.

Those skilled in the art may be further ware of that the units and algorithm steps in each example described in conjunction with the embodiments disclosed herein may be implemented by using electronic
20 hardware, computer software or a combination of the two. For a clear understanding of the interchangeability between the hardware and the software, the composition and steps of each example are described by

function in general in the description above. Whether these functions are executed in a form of hardware or software depends on the specific application of the technical solution and design constraints. Those skilled in the art may implement the described functions by using different manners for each specific application, but such implementation should not be construed as exceeding the scope of the present invention.

The steps of the methods or algorithms described in conjunction with the embodiments disclosed herein may be implemented by using hardware, software modules executed by a processor, or a combination of the two. The software modules may be placed in a random-access memory (RAM), an internal memory, a read-only memory (ROM), an electric programmable ROM, an electric erasable programmable ROM, a register, a hard disk, a removable magnetic disk, a CD-ROM, or storage mediums in any other forms as commonly known in the technical field.

The objects, technical solutions and advantageous effects of the present invention are further illustrated in detail with the specific embodiments described above. It should be understood that the description above only involves the specific embodiments of the present invention and is not intended to limit the protection scope of the present invention. Any modifications, equivalent substitutions, improvements and the like made within the spirit and principle of the present invention should be construed as being included within the protection scope of the present invention.

CLAIMS

1. A method for quantum key distribution in which participants include a first party and a second party, the method comprising:

the first party preparing a coherent pulse having a first optical intensity
5 and a first phase, and transmitting the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

the second party receiving the coherent pulse and preparing a local oscillator pulse having a second optical intensity and a second phase, and
10 inputting the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

the second party comparing the measurement result with a first
15 threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, determining a second key bit corresponding to the first key bit at the second party, and releasing the second random value to the first party; and

the first party determining whether to flip the first key bit based on the
20 first random value and the second random value.

2. The method of claim 1, further comprising:

if the measurement result does not satisfy the preset relation with the

first threshold, abandoning the determination of the second key bit corresponding to the first key bit at the second party.

3. The method of claim 1, wherein the first optical intensity is randomly selected from multiple preset intensity values.

5 4. The method of claim 1, wherein the first phase is expressed as:

$$\phi_i = \phi_i^a + \pi\kappa_a^i$$

where ϕ_i denotes the first phase, ϕ_i^a denotes the first random value, and κ_a^i denotes the first key bit.

5. The method of claim 1, wherein the first random value is randomly
10 selected by the first party from $\frac{2\pi}{D}k$ ($k=0,1,\dots,D-1$; D is a natural number) and the second random value is randomly selected by the second party from $\frac{2\pi}{D}k$ ($k=0,1,\dots,D-1$; D is a natural number).

6. The method of claim 1, wherein the first threshold is greater than 0; and if the measurement result satisfies a preset relation with the first
15 threshold, determining a second key bit corresponding to the first key bit at the second party comprises: if the measurement result is greater than the first threshold, determining the second key bit to be 0.

7. The method of claim 1, wherein the first threshold is greater than 0; and if the measurement result satisfies a preset relation with the first
20 threshold, determining a second key bit corresponding to the first key bit at

the second party comprises: if the measurement result is less than the negative of the first threshold, determining the second key bit to be 1.

8. The method of claim 1, wherein the first party determining whether to flip the first key bit based on the first random value and the second random value comprises: if the absolute value of the difference between the first
5 random value and the second random value falls within a preset range, flipping the first key bit.

9. A method for quantum key distribution in which participants include a first party and a second party, the method being executed by the first party,
10 comprising:

preparing a coherent pulse having a first optical intensity and a first phase, and transmitting the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

15 obtaining a second random value released by the second party upon determining that a measurement result satisfies a preset relation with a first threshold, the measurement result being obtained by the second party by inputting a local oscillator pulse having a second optical intensity and a second phase and the coherent pulse into a coherent detection module,

20 wherein the second optical intensity is greater than the first optical intensity and the second phase is determined according to the second random value; the first threshold being agreed upon by the first party and the second party;

and

determining whether to flip the first key bit based on the first random value and the second random value.

10. A method for quantum key distribution in which participants include
5 a first party and a second party, the method being executed by the second party, comprising:

receiving a coherent pulse having a first optical intensity and a first phase from the first party, wherein the first phase is determined according to a first random value held by the first party and a first key bit included in an
10 original key of the first party;

preparing a local oscillator pulse having a second optical intensity and a second phase, wherein the second optical intensity is greater than the first optical intensity of the coherent pulse, and the second phase is determined according to a second random value; inputting the coherent pulse and the
15 local oscillator pulse into a coherent detection module to obtain a measurement result; and

comparing the measurement result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, determining a second key bit
20 corresponding to the first key bit at the second party and releasing the second random value to the first party to enable the first party to determine whether to flip the first key bit based on the first random value and the second random value.

11. A system for quantum key distribution, comprising a first party and a second party as participants, wherein:

the first party is configured to prepare a coherent pulse having a first optical intensity and a first phase, and to transmit the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

the second party is configured to receive the coherent pulse and prepare a local oscillator pulse having a second optical intensity and a second phase, and to input the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result, wherein the second optical intensity is greater than the first optical intensity, and the second phase is determined according to a second random value;

the second party is further configured to compare the measurement result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, to determine a second key bit corresponding to the first key bit at the second party and to release the second random value to the first party; and

the first party is further configured to determine whether to flip the first key bit based on the first random value and the second random value.

12. An apparatus for quantum key distribution in which participants include a first party and a second party, the apparatus being disposed at the first party, comprising:

a preparation unit configured to prepare a coherent pulse having a first optical intensity and a first phase, and to transmit the coherent pulse to the second party, wherein the first phase is determined according to a first random value and a first key bit included in an original key of the first party;

5 an obtention unit configured to obtain a second random value released by the second party upon determining that a measurement result satisfies a preset relation with a first threshold, the measurement result being obtained by the second party by inputting a local oscillator pulse having a second optical intensity and a second phase and the coherent pulse into a coherent
10 detection module, wherein the second optical intensity is greater than the first optical intensity and the second phase is determined according to the second random value; the first threshold being agreed upon by the first party and the second party; and

a determination unit configured to determine whether to flip the first
15 key bit based on the first random value and the second random value.

13. An apparatus for quantum key distribution in which participants include a first party and a second party, the apparatus being disposed at the second party, comprising:

a measurement unit configured to receive a coherent pulse having a first
20 optical intensity and a first phase from the first party, wherein the first phase is determined according to a first random value held by the first party and a first key bit included in an original key of the first party; to prepare a local oscillator pulse having a second optical intensity and a second phase, wherein

the second optical intensity is greater than the first optical intensity of the coherent pulse, and the second phase is determined according to a second random value; and to input the coherent pulse and the local oscillator pulse into a coherent detection module to obtain a measurement result; and

- 5 a determination unit configured to compare the measurement result with a first threshold agreed upon by the first party and the second party; if the measurement result satisfies a preset relation with the first threshold, to determine a second key bit corresponding to the first key bit at the second party and release the second random value to the first party to enable the first
- 10 party to determine whether to flip its first key bit based on the first random value and the second random value.