# SYSTEMS AND METHODS FOR ABNORMALITY DETECTION IN QUANTUM KEY DISTRIBUTION

## TECHNICAL FIELD

The present disclosure relates to the security of quantum key distribution and, particularly, systems and methods for abnormality detection in quantum key distribution systems.

## BACKGROUND

Quantum key distribution (QKD) is a method for establishing shared secret keys between two remote parties. In its most basic form, a prepare-and-measure type QKD protocol involves the use of a QKD system, comprising at least two devices, namely, a transmitter and a receiver, transmitting and receiving light carrying quantum information over a quantum channel. They may be referred to as a QKD device hereafter.

Although the theoretical security of QKD has been proven mathematically, the overall security of real-world QKD systems depends on the implementation. An important security assumption commonly accepted by QKD users is that the QKD system is correctly implemented, trustworthy, and that its properties and operations have not been tampered or modified by malicious actors. For use cases requiring high security assurance, this security assumption should be validated.

QKD users may have concerns about the integrity of QKD systems during operation as there may be attackers exploiting undiscovered vulnerabilities, backdoors, or unexpected component failures that compromise security. QKD systems may also malfunction in a way that compromises security, for example, when there is a software bug. It is unclear today how to test or monitor the integrity of QKD systems in practice.

The detection of abnormalities can be a useful means to uncover an ongoing attack or identify a malfunctioning QKD system. This is because, in general, QKD systems tend to behave abnormally when experiencing an attack or when they malfunction.

However, QKD users today lack the means to detect abnormalities in QKD systems during operation since there are neither established methods nor tools readily available. Hence, it is desirable to provide abnormality detection systems and methods to satisfy the needs of QKD

users who wish to test or monitor the integrity of QKD during operation for greater security assurance.

SUMMARY

Disclosed herein are systems and methods for detecting abnormalities during QKD operation. Central to the disclosed systems and methods is the concept of abnormality detection testing which may involve intentionally applying a change to light in the quantum channel, collecting or receiving relevant data associated with the applied change, processing the data, and detecting abnormality from a discrepancy or deviation from expected behaviour that could be due to an ongoing attack or system malfunction. The abnormality may be detected from noticing or identifying anomalies in the data associated with the applied change.

In an example embodiment, the change is not applied to the QKD device or a component within a QKD device or light within a QKD device, even though the primary objective is to detect abnormality in a QKD system. The disclosed systems and methods may, therefore, be advantageous and practical because they may enable abnormalities of a QKD system to be detected from the outside of the QKD system, thus allowing the testing and monitoring of the integrity of a QKD system during operation without needing access to the internal of the QKD devices. The disclosed systems and methods may also be used to detect abnormalities in the quantum channel. For example, changes to the total optical path length or the total optical attenuation are abnormalities that may be the result of an attacker tampering with the quantum channel.

According to one aspect, the type of the change, the timing of applying the change, the duration of applying the change, the magnitude of the change, and/or the pattern of the change applied to the light in the quantum channel may be made unpredictable to any attacker or intentionally not made known to one or more components of the QKD system before or during applying the change. Consider the following scenario in which a QKD device is controlled by malicious code and behaving in an abnormal way such that the security of the quantum keys is compromised. Suppose the malicious code knows when an abnormality detection test is going to happen or the type and duration of a change that will be applied to the light in the quantum channel, the malicious code may instruct the QKD device under its control to halt its security-compromising behaviour and temporarily revert to normal behaviour during the test, thus defeating the test. Therefore, it is desirable for the abnormality detection system to select the type, timing, duration, magnitude, and/or the pattern of the change to be applied to the light in the quantum channel in a randomized, unpredictable, and/or independent way such

that the QKD system or any attacker cannot counter the abnormality detection test by prediction, estimation or guessing correctly.

In an example embodiment, the abnormality detection system may not provide any information or send any query to the QKD system that may leak the intent of carrying out a test. In the case where raw data is obtained from the QKD system, it is preferable that the abnormality detection system sends its request only after the test has ended or in some way that does not leak the information of the test, the information including the characteristics of the change to be applied to the light in the quantum channel, for example, the timing of applying the change or the duration of the application of the change.

Another aspect is that the abnormality detection system, comprising one or more optoelectronic modules and computing systems for carrying out abnormality detection tests, may be operated independently and, preferably, be physically separated from the QKD devices. In practice, the optoelectronic modules and computing systems may be located together with the QKD devices in the same secure location, but it is preferable that they do not come under the influence of the QKD devices which are under test. Each optoelectronic module may contain its own processor or processing unit, or be integrated with a computing system for control functions and data processing.

According to another aspect, a method is provided for detecting abnormality in QKD comprising the following steps. First, a change is applied to the light in the quantum channel, wherein the type of the change, the timing of applying the change, the duration of applying the change, the magnitude of the change, and/or the pattern of the change are not made known to the QKD system before or during applying the change. The change may involve removing an amount of light from the quantum channel, adding an amount of light into the quantum channel, or modulating a property of the light in the quantum channel, or any combination of them. Depending on the quantum information encoding, the property of the light may be optical properties of the light, including intensity, phase, time delay, wavelength, frequency, polarization, etc. Details on how and when to apply the change may either be provided via at least one processing unit to the optoelectronic modules applying the change, wherein the at least one processing unit is in the optoelectronic modules or in a computing system preferably operating independently from the QKD system. The optoelectronic modules may receive clock signals from the QKD devices for timing synchronization. This may be necessary when applying a time-dependent change to a property of the light in the quantum channel. For example, a change involving a distinct modulation level applied to individual light pulses carrying quantum information in the quantum channel would require accurate timing

synchronization. The optoelectronic modules should not send a request for clock signals only when an abnormality detection test is about to be performed because this may give information to the QKD devices about the timing of the test. Instead, it is preferred that the clock signals are provided to the optoelectronic modules continuously.

During a typical abnormality detection test, data associated with the applied change are collected or received, and at the end of the test, they may be used to obtain the value of a property of the QKD system. The property of the QKD system may be the mean photon number of the light sent from the transmitter, the total optical attenuation experienced by the light in the quantum channel, the total optical path length traversed by the light in the quantum channel, the amount of noise in the quantum channel, the quantum bit-error rate (QBER), the key rate, etc., depending on the test. The obtained value may be compared against an expected value or a range of values or past obtained values of the property of the QKD system, and a discrepancy or deviation provides the detection of abnormality.

In some embodiments, there may be a requirement for the abnormality detection system to request for raw data, such as the encoding basis and bit-value choices, the decoding basis choices, or the detection timestamps and the measured bit-values, from the QKD system for the abnormality detection system to obtain the value of a desired property of the QKD system. For example, when an abnormality detection test includes many short durations of changes applied at random timings within a time range, the QBER can be calculated from the raw data recorded during the short durations. Another example is where encoding at the transmitter involves using light pulses of different types, for example, signal pulses and decoy pulses having different optical intensities, with different occurrence probabilities. In this case, it would be necessary for an abnormality detection system to receive the relevant raw data recorded during test duration from the QKD system so that it may obtain the mean-photon number value for each type of light pulses for detecting abnormality in the optical intensities and occurrence probabilities.

It is preferable that the following two conditions are satisfied. Firstly, the raw data is obtained from the QKD system in a way that it does not leak the intent to carry out a test. This is to prevent the QKD system or any attacker from predicting when a test will happen and rendering the abnormality detection test ineffective. Secondly, the final secret key is preferably not derived from the raw key bits associated with the raw data obtained by the abnormality detection system. The raw key bits associated with the raw data provided to the abnormality detection system may be discarded and not used for secret key generation for security.

According to another aspect, it is provided an abnormality detection system and method for detecting a known basis attack, in which an attacker having knowledge of the encoding basis at the transmitter performs an error-free intercept-resend attack on the light carrying quantum information in the quantum channel. An embodiment of the abnormality detection system comprises a first optoelectronic module and a second optoelectronic module of the one or more optoelectronic modules. The first optoelectronic module is preferably placed near the transmitter, while the second optoelectronic module is preferably placed near the receiver. During an abnormality detection test, the first optoelectronic module applies a first modulation to a property of the light in the quantum channel. Depending on the quantum information encoding, the property may be optical intensity, phase, time delay, wavelength, frequency, polarization, etc. At the same time, the second optoelectronic module applies a second modulation that reverses or cancels the first modulation. To the QKD system, the first modulation and the second modulation do not lead to a net effect since they cancel each other. The QBER should not be affected. Take phase encoding for example, the first optoelectronic module and the second optoelectronic module apply a random yet opposite phase modulation during test. If any attacker located at any point along the quantum channel between the two optoelectronic modules attempts to carry out a known-basis intercept-resend attack, the attack will not lead to error-free eavesdropping and the resultant QBER will be high since the attacker does not know the random phase modulation applied on the light by the first optoelectronic module. Another example is random time-delay modulation applied by the first optoelectronic module and reversed by the second optoelectronic module. Since the attacker cannot predict the random time delay applied by the first optoelectronic module, a known basis attack cannot be performed without causing errors under such a condition. Therefore, the method obtains the QBER during the application of the first modulation and the second modulation, wherein an increase in the QBER provides the detection of abnormality that reveals the presence of a known basis attack. Preferably, the modulation is applied in randomly timed short durations to avoid noticeably affecting the overall QBER. Detection of the known-basis attack is possible by processing raw data obtained from the QKD system to obtain the QBER of the raw key bits recorded during the times when modulation is applied and detecting a deviation from the expected QBER value.

According to another aspect, it is provided a system and method for detecting abnormality in QKD due to device malfunctioning or corruption by malicious code. During an abnormality detection test, an optoelectronic module preferably located near the transmitter removes a proportion of the light, optionally the amount of light removed is a small percentage, for example 1%, from the quantum channel and measures the mean photon number of the removed light. If the mean photon number value deviates from an expected value or range of

values or past obtained values, it could be due to QKD device malfunctioning or corruption by malicious code.

According to another aspect, it is provided a system and method for detecting abnormality caused by a photon detector blinding attack where an attacker sends an intense laser into the receiver. During an abnormality detection test, an optoelectronic module preferably placed near the receiver applies an intensity modulation to the light in the quantum channel, preferably wherein the intensity modulation is randomly determined or intentionally made unpredictable to any attacker. If there is an ongoing photon detector blinding attack, the intensity modulation would disrupt the blinding effect by the laser and result in an increase in the QBER. If the QBER value recorded during the test deviates from an expected value or range of values or past obtained values, it indicates that the receiver is undergoing a photon detector blinding attack. If a count rate deviates from an expected value or range of values or past obtained values, abnormality in the QKD system is indicated.

According to another aspect, it is provided a system and method for detecting abnormality in the total optical path length traversed by the light in the quantum channel or the total optical attenuation experienced by the light in the quantum channel. During an abnormality detection test, a first optoelectronic module preferably placed near the transmitter adds an amount of light, the light may be of the same wavelength or different wavelength as the light carrying the quantum information, into the quantum channel, and a second optoelectronic module preferably placed near the receiver removes an amount of light from the quantum channel and measures the photon arrival time and mean photon number of the removed light. The optical path length traversed by the light in the quantum channel and the optical attenuation experienced by the light in the quantum channel can be obtained by processing the measurement data. A deviation from expected values or range of values or past obtained values would indicate the presence of an abnormality. Although this may not be an abnormality of the QKD devices, it is useful for QKD users to monitor any changes to the total optical path length and the total optical attenuation experienced by the light in the quantum channel as such an abnormality may be the result of an ongoing attack on the QKD system.

According to another aspect, it is provided a system and method for detecting an abnormality in the QKD system's responsiveness to changes in QBER that may be caused by eavesdropping. During an abnormality detection test, an optoelectronic module performs emulated eavesdropping that deliberately increases the QBER for one or more time durations, which are preferably not made known to the QKD system before or during the performing of

the emulated eavesdropping. If the QKD system does not record an increase in the QBER, or the key rate does not decrease during the test, an abnormality is detected.

Preferably, a test is performed in randomly timed short durations to avoid noticeably affecting the operation of the QKD, especially the overall QBER, and also to prevent malicious actors from predicting, estimating, or guessing correctly the time and duration of the test. Only the abnormality detection system knows which raw key bits fall within the randomly timed short durations during which the change is applied. This prevents a compromised QKD system from evading detection as it will have no knowledge of the time range during which an abnormality detection test is being performed. Detection of abnormality may be possible by obtaining and processing raw data recorded within the time range of the test, for example, to calculate the QBER of those raw key bits recorded during the short durations and determining whether there is a significant deviation from the expected QBER value.

According to an aspect of the present disclosure, a method is provided for detecting abnormality in a quantum key distribution (QKD) system. The method comprises applying a change to light in a quantum channel of the QKD system, wherein one or more characteristics of the change are not made known to one or more components of the QKD system before or during applying the change, collecting or receiving data associated with the applied change, obtaining a value of a property of the QKD system using the collected or received data, comparing the obtained value to an expected value of the same property, and identifying a discrepancy or deviation in the obtained value, wherein a discrepancy or deviation indicates abnormality in the QKD system.

In an embodiment, the one or more characteristics of the change comprise the type of the change, the timing of applying the change, the duration of applying the change, the magnitude of the change, and/or the pattern of the change; and/or wherein, at least one of the one or more characteristics of the change is determined randomly or intentionally made unpredictable to any attacker; and/or wherein, the change comprises one or more of the following:

- removing an amount of light from the quantum channel,
- adding an amount of light into the quantum channel,
- modulating a property of the light in the quantum channel, the property of the light comprising one or more of the optical properties of the light, including optical intensity, phase, time delay, wavelength, frequency, or polarization of the light; and/or

wherein, the change is applied for short durations, preferably randomly timed, to avoid noticeably affecting the operation of the QKD system; and/or wherein, the received data includes one or more of encoding basis choices, bit-value choices, decoding basis choices,

detection timestamps, and/or detected bit values, and raw key bits associated with the received data are preferably not used by the QKD system for secret key generation; and/or wherein, the expected value of the property of the QKD system comprises one or more of an estimated, modelled, or simulated value, or a range of values, or past obtained values of the same property; and/or wherein, the property of the QKD system comprises one or more of the following:

- a mean photon number of the light sent from a transmitter;
- a total optical attenuation experienced by the light in the quantum channel;
- a total optical path length traversed by the light in the quantum channel;
- an amount of noise in the quantum channel,
- a quantum bit-error rate (QBER), or
- a key rate.

In an embodiment, the method further comprises providing one or more characteristics of the change via at least one processing unit to one or more optoelectronic modules applying the change wherein the at least one processing unit is in the one or more optoelectronic modules or in a computing system preferably operating independently from the QKD system.

In an embodiment, the method further comprises providing a time and duration associated with the short durations to the QKD system after applying the change.

In an embodiment, the method further comprises the steps of applying a first modulation to a property of the light in the quantum channel of the QKD system, the first modulation applied via a first optoelectronic module, and applying a second modulation to a property of the light in the quantum channel of the QKD system, the second modulation applied via a second optoelectronic module, wherein the second modulation is configured to reverse or cancel the first modulation, and obtaining the QBER during the time when the first modulation and the second modulation are applied, wherein an increase in the QBER during the applying of the first modulation and the second modulation provides the detection of abnormality.

In an embodiment, the method further comprises the steps of removing a proportion of light from the quantum channel via an optoelectronic modules preferably located near a transmitter of the QKD system, optionally wherein the proportion of light removed is 1%, measuring the mean photon number of the removed light, and identifying a deviation in the mean photon number value from an expected value or range of values or past obtained values, wherein the deviation indicates abnormality in the QKD system.

In an embodiment, the method further comprises the steps of applying an intensity modulation to light in a quantum channel of the QKD system via an optoelectronic modules preferably placed near a receiver of the QKD system, preferably wherein the intensity modulation is randomly determined or intentionally made unpredictable to any attacker; and measuring if a count rate deviates from an expected value or range of values or past obtained values, wherein, a deviation indicates abnormality in the QKD system.

In an embodiment, the detection of abnormality indicates that the receiver is undergoing a photon detector blinding attack.

In an embodiment, the method further comprises adding an amount of light into the quantum channel of the QKD system, removing an amount of light from the quantum channel of the QKD system, measuring a photon arrival time and mean photon number of the removed light, and processing the measured data to obtain the optical path length traversed by the light in the quantum channel and the optical attenuation experienced by the light in the quantum channel, wherein a deviation from an expected value or range of values or past obtained values indicates abnormality in the QKD system.

In an embodiment, the light added is preferably of different wavelength as the light carrying the quantum information in the QKD system, although it may be acceptable to use light of the same wavelength.

In an embodiment, the method further comprises the steps of performing an emulated eavesdropping to increase the QBER of the QKD system for one or more time durations, wherein the one or more time durations are preferably not made known to the QKD system before or during performing the emulated eavesdropping; and obtaining from the QKD system data taken during the one or more time durations and processing the obtained data to determine if the QBER increased during the one or more time durations, wherein the absence of an increase in the QBER indicates abnormality in the QKD system.

In an embodiment, the one or more time durations are preferably not made known to the QKD system before or during the performing of emulated eavesdropping.

In an embodiment, the one or more time durations are randomly timed short durations to avoid noticeably affecting the operation of the QKD system.

According to another aspect of the present disclosure, a method for detecting abnormality in a QKD system, wherein one or more of the methods according to the above embodiments of the first aspect are implemented individually, in parallel, in series, or in any combination.

According to another aspect of the present disclosure, a system is provided for detecting abnormality in a QKD transmission, the system comprises one or more optoelectronic modules configured to apply a change to light in a quantum channel of the QKD system, wherein one or more characteristics of the change are not made known to one or more components of the QKD system before or during applying the change, and at least one processing unit configured to collect or receive data associated with the applied change, obtain a value of a property of the QKD system using the collected or received data, compare the obtained value to an expected value of the property of the QKD system, and identify discrepancy or deviation in the obtained value, wherein the discrepancy or deviation indicates abnormality in the QKD system.

In an embodiment, the one or more characteristics of the change comprise the type of the change, the timing of the change, the duration of applying the change, the magnitude of the change, and/or the pattern of the change; and/or wherein, at least one of the one or more characteristics of the change is determined randomly or intentionally made unpredictable to any attacker; and/or wherein the change comprises one or more of the following:

- removing an amount of light from the quantum channel,
- adding an amount of light into the quantum channel,
- modulating a property of the light in the quantum channel, the property of the light comprising one or more of the optical properties of the light, including optical intensity, phase, time delay, wavelength, frequency, or polarization of the light; and/or

wherein, the change is applied for short durations, preferably randomly timed, to avoid noticeably affecting the operation of the QKD system; and/or wherein, the received data includes one or more of encoding basis choices, bit-value choices, decoding basis choices, detection timestamps, and/or detected bit values, wherein one or more raw key bits associated with the received data are preferably not used by the QKD system for secret key generation; and/or wherein, the expected value of the property of the QKD system comprises one or more of an estimated, modelled, or simulated value, or a range of values, or past obtained values of the same property; and/or wherein, the property of the QKD system comprises one or more of the following:

- a mean photon number of the light sent from a transmitter;
- a total optical attenuation experienced by the light in the quantum channel;
- a total optical path length traversed by the light in the quantum channel;
- an amount of noise in the quantum channel,

- a quantum bit-error rate (QBER), or
- a key rate.

In an embodiment, the at least one processing unit is configured to provide the one or more characteristics of the change to the one or more optoelectronic modules applying the change, and wherein the at least one processing unit is in the one or more optoelectronic modules or in a computing system preferably operating independently from the QKD system.

In an embodiment, the system further comprises a first optoelectronic module preferably located near a transmitter of the QKD system, configured to apply a first modulation to apply a first modulation to a property of the light in the quantum channel of the QKD system, and a second optoelectronic module preferably located near a receiver of the QKD system, configured to apply a second modulation to a property of the light in the quantum channel of the QKD system, wherein the second modulation is configured to reverse or cancel the first modulation, and wherein, the at least one processing unit configured to obtain the QBER during the application of the first modulation and the second modulation, wherein an increase in the QBER provides a detection of abnormality. The QBER may be received from the QKD system or calculated based on raw data received from the QKD system or obtained via alternative means.

In an embodiment, the detection of abnormality reveals the presence of a known basis attack.

In an embodiment, the system further comprises at least one optoelectronic module, preferably located near a transmitter of the QKD system, configured to remove a proportion of light from the quantum channel, optionally wherein the proportion of light removed is 1%, measure the mean photon number of the removed light, and at least one processing unit, configured to identify a deviation in the mean photon number value from an expected value or range of values or past obtained values, wherein the deviation indicates abnormality in the QKD system.

In an embodiment, the one or more optoelectronic modules are configured to apply an intensity modulation to the light in the quantum channel of the QKD system via an optoelectronic modules preferably placed near the receiver of the QKD system, preferably the intensity modulation is randomly determined or intentionally made unpredictable to any attacker; and wherein the at least one processing unit is configured to measure if a count rate deviates from an expected value or range of values or past obtained values, wherein a deviation indicates abnormality in the QKD system.

In an embodiment, the one or more optoelectronic modules are configured to add an amount of light, into the quantum channel of the QKD system, remove an amount of light from the quantum channel of the QKD system, measure a photon arrival time and mean photon number in of the removed light, and wherein the at least one processing unit is configured to process the measured data to obtain the optical path length traversed by light in the quantum channel and the optical attenuation experienced by light in the quantum channel, wherein a deviation from an expected value or range of values or past obtained values indicates an abnormality in the QKD system.

In an embodiment, the one or more optoelectronic modules are configured to perform an emulated eavesdropping to increase the QBER of the QKD system for one or more time durations, wherein the one or more time durations are preferably not made known to the QKD system before or during the performing of the emulated eavesdropping, and wherein the at least one processing unit is configured to obtain from the QKD system data taken during the one or more time durations, process the obtained data to determine if the QBER increased during the one or more time durations, wherein the absence of an increase in the QBER indicates abnormality in the QKD system.

According to another aspect of the present disclosure a system for detecting abnormality in a quantum key distribution (QKD) system, wherein one or more of the systems according to the above embodiments of the third aspect are implemented individually, in parallel, in series, or in any combination

BRIEF DESCRIPTION OF THE DRAWINGS

In the following, embodiments of the present disclosure will be described as non-limiting examples with reference to the accompanying drawings in which:

Fig. 1A illustrates a QKD link of the prepare-and-measure type;

Fig. 1B illustrates a flow chart of a method according to an example embodiment as disclosed herein;

Fig. 2 illustrates an example embodiment of a QKD link equipped with an abnormality detection system;

Fig. 3 illustrates an example embodiment of an abnormality detection system with inter-link connection spanning two QKD links;

Fig. 4 illustrates an example embodiment of a QKD link equipped with an abnormality detection system for detecting known-basis attack;

Fig. 5 illustrates an example embodiment of a QKD link equipped with an abnormality detection system for detecting known-basis attack based on time-delay modulation; and

Fig. 6 illustrates an example embodiment of a concept of randomly timed short duration transmission.

DETAILED DESCRIPTION

The present disclosure relates to the security of quantum key distribution (QKD) and, particularly, systems and methods for abnormality detection as a means of testing and monitoring the integrity of quantum key distribution systems.

A typical QKD protocol involves two stages, a quantum transmission stage followed by a classical post-processing or key distillation stage. Fig. 1A shows the schematic 10 of a conventional QKD link that implements a prepare-and-measure QKD protocol. During the quantum transmission stage, a transmitter 12 encodes quantum information onto light and sends the light carrying the quantum information over a quantum channel 14 to a receiver 16. The encoding may be performed on either discrete or continuous variables of the light. The receiver 16 decodes the quantum information by measuring the received light. Depending on the type of encoding, the measurement may be based on photon detection or homodyne detection. For illustration, the descriptions hereafter assume encoding onto discrete variables of light and measurement based on photon detection. The light may be in the form of periodic pulses or continuous waves. For simplicity, the descriptions hereafter assume quantum transmission using weak light pulses, however it will be understood that any quantum transmission mechanism may be utilised in the systems and methods disclosed herein.

During the subsequent key distillation stage, both the transmitter 12 and the receiver 16 communicate over an authenticated classical communication channel, commonly called service channel 18 to perform basis reconciliation to obtain raw key bits and post-processing steps including error correction on the raw key bits and privacy amplification on the error-corrected key bits to obtain the final shared secret keys, also called quantum keys or QKD

keys. The quantum keys may then be supplied to key management servers or agents that coordinate key usage among key-consuming appliances such as encryptors.

The number of quantum key bits that can be distilled from a block of raw key bits depends largely on the quantum bit-error rate (QBER), which is used to upper bound the amount of information leakage to potential eavesdroppers. If the QBER is found to exceed a security threshold, the raw key bits are discarded, and no quantum key can be produced.

In general, a QKD system tends to behave abnormally when attacked or when it malfunctions. For example, a malfunctioning transmitter may send out more photons than usual, or a corrupted QKD system may become irresponsive to QBER changes. Such abnormalities may indicate that the security of the keys is compromised. It is envisaged that an abnormality detection system may carry out one or more abnormality detection tests to detect such abnormalities, thus enabling QKD users to test or monitor QKD system integrity during operation.

Fig. 1B illustrates a flow chart of a method 100 according to an example embodiment as disclosed herein. The method 100 may be suitable for detecting abnormality in a quantum key distribution (QKD) system, such as the example systems embodiments disclosed in Fig. 2 to Fig. 5 as set out herein.

The method 100 may comprise applying at 110 a change to light in a quantum channel of the QKD system.

In an example embodiment, one or more characteristics of the change made at step 110 are not made known to one or more components of the QKD system before or during applying the change.

The method 100 may further comprise collecting or receiving at 120 data associated with the applied change, obtaining at 130 a value of a property of the QKD system using the collected or received data, and comparing at 140 the obtained value to an expected value of the same property.

In an example embodiment, the method 100 may identify at 150 a discrepancy or deviation in the calculated value calculated at step 130 compared to the expected value during comparison step 140.

Fig. 2 shows a generic configuration 200 of a QKD link equipped with an abnormality detection system for detecting abnormalities caused by malicious attacks on the QKD system or malfunctioning of the QKD system. An abnormality detection system of the present embodiment comprises at least one optoelectronic module placed on the quantum channel and at least one computing system. The computing system may be integrated into the optoelectronic module, or a standalone server communicatively connected to the optoelectronic module. Multiple optoelectronic modules may communicate with one another to coordinate an abnormality detection test.

It is advantageous that the abnormality detection system operates from outside of a QKD system to separate its security requirements from that of the QKD system. It is further advantageous to have the abnormality detection tests performed at random timings, without the QKD system knowing, to prevent sophisticated attacks from using this knowledge to evade detection. Nevertheless, it is envisaged that in some embodiments having a lower security requirement, the abnormality detection system may be integrated into the QKD system.

The optoelectronic modules in an abnormality detection system are primarily used to cause a change to the light in the quantum channel during an abnormality detection test at randomly chosen timings and durations. The change may involve the removal of an amount of light from the quantum channel, the addition or insertion of an amount of light into the quantum channel, or the modulation of a characteristic of the light in the quantum channel. The amount of light removed or added may be randomized. The characteristic of the light that is modulated may be the optical intensity, phase, polarization, frequency, time delay, etc. The computing system has at least one processor or processing unit, for carrying out data processing, one or more data storage for storing data, and at least one communication interface to enable it to communicate data with the optoelectronic modules, other computing systems, and the QKD system.

Apart from applying a change to the light in a quantum channel, an optoelectronic module may include other functionalities such as collecting data associated with the change applied to the light. For example, an optoelectronic module may comprise one or more photosensitive devices, such as photon detectors that detect the photon count rate of the light removed from the quantum channel or photodiodes that measure the optical power of the removed light. The computing system may receive data from the optoelectronic modules, obtain data from the QKD system, such as QBER and key rate, and may further process the received data to determine the presence of an abnormality or abnormalities. In some embodiments, the data

are not processed by the computing system but passed to an operator or some other party for processing and carrying out abnormality detection.

In general, different types of abnormalities may require different tests for their detection, and there may be no single test that can detect all types of abnormalities of concern. However, in an example embodiment, an optoelectronic module or system as disclosed herein may be configured for detecting multiple abnormalities or combine two or more abnormality detection tests into one test. It is advantageous to implement an abnormality detection system capable of carrying out various abnormality detection tests to cover a wide range of different abnormalities.

In the generic configuration 200 shown in Fig. 2, the QKD link includes a transmitter 202, a receiver 214, a quantum channel comprising two segments 206, 210, and a service channel 218. The abnormality detection system includes a computing system 228 and three optoelectronic modules 204, 208, and 212. The first optoelectronic module 204 is placed near the transmitter 202, the second optoelectronic module 208 is placed at a secure location along the quantum channel, and the third optoelectronic module 212 is placed near the receiver 214. Each optoelectronic module may be configured to insert light into, remove light from, modulate the light in the quantum channel, or apply any change to the light in the quantum channel. In some embodiments, an optoelectronic module may have a shutter to block the light in the quantum channel during a test. All three optoelectronic modules, 204, 208, and 214, may be communicatively connected to a computing system 228 via communication links 220, 222, and 224, respectively. The computing system 228 may be located near any of the optoelectronic modules. The computing system 228 may be communicatively connected to the transmitter 202 and the receiver 214 via communication links 216 and 226, respectively.

It will be understood that it is not a requirement to have exactly three optoelectronic modules in an abnormality detection system or method as disclosed herein. In some embodiments, only one optoelectronic module, for example only 204 or only 212 may be used. In some other embodiments, two optoelectronic modules, for example 204 and 212, are used. Yet in some other embodiments, more than three optoelectronic modules may be used. Examples are provided below.

In one embodiment, the abnormality detection system has only one optoelectronic module 204. The optoelectronic module 204 is co-located with the transmitter 202 in a secure location. Preferably, the optoelectronic module 204 is not part of the transmitter 202. According to an aspect, it is preferable that the QKD system does not influence the operation of the abnormality

detection system. Therefore, it is preferred that the optoelectronic module 204 and the computing system 228 receive only relevant data but not any instruction from the QKD system such that the abnormality detection system may perform testing independently. The communication links, 216 and 220, may transfer data directly over a cable such as a serial cable. On the other hand, the communication link 226 connecting the receiver 214 and the computing system 228 may traverse a public network, and therefore, the communicated data may be authenticated and secured via a standard secure data transfer protocol such as TLS (Transport Layer Security). The data may also be secured using quantum keys if deemed necessary.

During an abnormality detection test, the optoelectronic module 204 applies a change to the light coming from the transmitter 202. The change may be the removal of a proportion of the light or the addition of light or the modulation of a characteristic of the light. Neither the type, timing, duration, magnitude, nor pattern of the change may be revealed to the QKD devices 202 and 214. It is preferred that the timing, duration, magnitude, or pattern of the change is determined randomly such that it cannot be predicted by any attacker. After the test has ended, depending on the test, the computing system 228 may obtain data associated with the applied change from the optoelectronic module 204 or the QKD devices 202 and 214 via the communication links 220, 216, and 226, respectively, and process the data to determine if there was an abnormality. The optoelectronic module 204 may provide information regarding the time and duration of the test, the QKD devices 202 and 214 may provide the QBER values recorded within the duration of the test.

In another embodiment, the abnormality detection system comprises two optoelectronic modules 204 and 212 and the computing system 228. The first optoelectronic module 204 is placed near the transmitter 202, while the second optoelectronic module 212 is placed near the receiver 214. This configuration may be used to perform a variety of abnormality detection tests. Two examples are given below.

One example of an abnormality detection test utilizing this configuration involves the use of an optical intensity modulator in the first optoelectronic module 204 and the use of a 99:1 optical splitter and a photon detector in the second optoelectronic module 212. During the test, the optical intensity modulator in the first optoelectronic module 204 modulates the intensity of the light coming from the transmitter 202 at randomly selected timings and durations to deliberately reduce the count rate. The 99:1 optical splitter removes 1% of the incoming light and directs the removed light to the photon detector, which records photon detection events. After the test has ended, the computing system 228 obtains from the first optoelectronic

module 204 the timings and durations when the optical intensity modulation was applied, and from the second optoelectronic module 212 the raw data of photon detection events recorded during the test. It is possible to calculate the photon count rates with or without modulation applied. If the photon count rates do not correctly reflect the optical modulation applied at the first optoelectronic module 204, this would be a discrepancy and an abnormality is detected. The computing system 228 may also obtain the photon detection rate recorded by the receiver 214. If the photon detection rate does not correspond to the optical modulation applied at the first optoelectronic module 204, an abnormality is detected.

Another example of an abnormality detection test utilizing this configuration involves the use of a pair of optical phase modulators, one in each of the optoelectronic modules 204 and 212. During the test, the first optoelectronic module 204 applies a randomly selected phase modulation to the light exiting the transmitter 202 for a randomly determined duration, while the second optoelectronic module 212 applies the opposite phase modulation to reverse the phase modulation applied by the first optoelectronic module 204. Such optical phase modulation operations do not affect the QBER of the QKD operation as phase shifts are reversible, and they do not involve any measurement that may disrupt the quantum information.

The timing for the two optical phase modulators to apply the opposite modulation is separated by the time needed for the light to travel from optoelectronic module 204 to optoelectronic module 212. For example, if the optical path length between the two optoelectronic modules 204 and 212 is L = 50 km, the time delay between the optical phase modulator of the optoelectronic module 204 applying the first phase modulation and the optical phase modulator of the optoelectronic module 212 applying the second phase modulation may be calculated from $L * n / c = 0.245$ ms, where c is the speed of light and $n = 1.47$ is the refractive index of optical fibre.

After the test has ended, the computing system 228 obtains from the QKD system the QBER and key rate recorded during the test. An abnormality is detected if found that the QBER increased, and the key rate dropped during the test. This is an abnormality because since the second phase modulation reverses the first phase modulation, the phase modulation applied by the two optoelectronic modules 204 and 212 should have no net effect on the QKD operation, and the QBER and the key rate should not be affected during the test. Thus, a significant increase in the QBER and a drop in the key rate is an abnormality that may indicate that the QKD link is undergoing an attack. To avoid leading to a noticeable increase to the QBER, the test may be performed for a series of randomly timed short durations, such that any attacker may remain unaware of the test. After the test has ended, the computing system

228 obtains from the QKD system the raw data recorded during all the randomly timed short durations and uses the raw data to calculate the overall QBER. The raw data obtained by the computing system may not be used for secret key generation.

The phase modulation in the above example may be replaced with other types of modulation, for example, polarization modulation, frequency modulation, time-delay modulation, etc. All these modulations may be randomly applied by the first optoelectronic module 204 and then reversed by the second optoelectronic module 212 after a time delay accounting for the time-of-flight of the light over the quantum channel, as described above.

It is envisaged that the two optoelectronic modules 204 and 212 coordinate over an encrypted and authenticated channel to apply the modulation correctly and synchronized, without the QKD system knowing that a test is being performed.

In another embodiment, the abnormality detection system comprises the computing system 228 and the optoelectronic module 212 that is co-located with the receiver 214. During an abnormality detection test, the optoelectronic module 212 applies a change to the light coming from the quantum channel 210 just before the light enters the receiver 214. The change may involve the removal or addition of light or modulation of the light. This is useful for detecting abnormalities that may arise when the integrity of the receiver 214 is compromised under an attack. Examples are given below.

One example of an abnormality detection test utilizing this configuration involves the use of a variable optical attenuator in the optoelectronic module 212. During the test, the variable optical attenuator applies an optical attenuation of a randomly determined magnitude at randomly selected timings to the light coming from the quantum channel 210. After the test has ended, the computing system 228 obtains from the optoelectronic module 212 the timings and the magnitude of the applied attenuation, and from the QKD system the timestamps of the detection events registered during the test. It is then straightforward to verify that the count rate is modulated by the applied attenuation during the test. If the count rate remains unchanged during the times when higher attenuation is applied, this would be a discrepancy from the expected result of a lower count rate, and an abnormality is detected.

Another example of an abnormality detection test utilizing this configuration involves the use of a noise source in the optoelectronic module 212. During the test, the noise source adds a randomly determined amount of noise at randomly selected timings to deliberately increase the number of detection errors. After the test has ended, the computing system 228 obtains

from the optoelectronic module 212 the timings when the noise was deliberated added, and from the QKD system the QBER and key rate recorded during the test. If the QBER and key rate had remained unchanged during the times when noise was added, this would be a discrepancy from the expected result of a higher QBER and lower key rate, and an abnormality is detected.

A third example of an abnormality detection test utilizing this configuration involves the use of an optical intensity modulator in the optoelectronic module 212. During the test, the optical intensity modulator modulates the intensity of the light coming from the quantum channel 210 at randomly selected timings and durations to deliberately reduce the count rate at the receiver 214. After the test has ended, the computing system 228 obtains from the optoelectronic module 212 the time duration when the optical intensity modulation was applied, and from the QKD system the detection timestamps recorded during the test. If the count rate had remained unchanged during optical modulation, this would be a discrepancy from the expected result of a lower count rate, and an abnormality is detected. The modulation may be applied in a series of short bursts at random selected timings such that the decrease in count rate is not obvious to the receiver 214. The computing system 228 knowing the duration and timing of each burst may aggregate the number of counts during the bursts from the detection timestamps data received from the receiver 214 to obtain the count rate during modulation.

It should be appreciated that all three of the embodiments described above may be combined within one optoelectronic module 212. The optoelectronic module may include an intensity modulator for modulating the intensity of the light in the quantum channel 210, an optical coupler placed after the intensity modulator for connecting a light source to the quantum channel 210 and tapping a percentage of the light from the quantum channel 210 for detection with one or more photosensitive devices such as photon detector or photodiode. The light source may be turned on only when testing the QBER responsiveness of the QKD system. The optical coupler may have a variable or fixed coupling ratio such as 99:1.

Consider an embodiment utilizing the configuration shown in Fig. 2. During an abnormality detection test, the optoelectronic module 204 sends reference light pulses into the quantum channel 206. The optoelectronic modules 208 and 212 each removes a predetermined proportion, for example 1%, of the light from the quantum channel segments 206 and 210, respectively, to measure the optical power and time-of-flight of the light pulses. If the measured optical power and time-of-flight values deviate from expected values or previously obtained values, an abnormality is detected. This abnormality may reveal unauthorized tampering with

the optical transmission line. In this example, there is no need for the computing system 228 to obtain data from the QKD devices.

In another embodiment utilizing the configuration shown in Fig. 2, the abnormality detection test involves the optoelectronic module 204 blocking all the light coming from the transmitter 202 using a shutter, while the optoelectronic modules 208 and 212 remove a predetermined proportion of the light from the quantum channel segments 206 and 210, respectively, to measure the noise level of each segment using a photon detector. After the test has ended, the computing system 228 obtains the count rates recorded by the optoelectronic modules 208 and 212 during the test. If the noise photon count rate, obtained from the difference between the photon count rate and the detector's dark count rate, is substantially higher than the expected range or previously recorded values for any of the segments, an abnormality is detected. This abnormality may reveal the presence of a noise source in the quantum channel.

Although a generic configuration of a QKD link equipped with an abnormality detection system is described above, it should not be construed as restrictive. For example, an abnormality detection system may be constructed to span multiple QKD links. Fig. 3 shows a configuration 300 in which the abnormality detection system has an inter-link connection and spans two QKD links. Such a configuration is advantageous in use cases where multiple QKD links form a QKD network.

In Fig. 3, the first QKD link comprises a first transmitter 302, a first quantum channel 306, a first receiver 314, and a first service channel 332. The second QKD link comprises a second transmitter 316, a second quantum channel 324, a second receiver 328, and a second service channel 346. The abnormality detection system comprises a computing system 354, a first optoelectronic module 304, a second optoelectronic module 308, a third optoelectronic module 322, a fourth optoelectronic module 326, and an inter-link connection comprising a first optical coupler 310, a first optical link 312, an optional fifth optoelectronic module 340, a second optical link 320, and a second optical coupler 318. The first optical coupler 310 and the second optical coupler 318 may be wavelength-division-multiplexing (WDM) couplers. The computing system 354 is communicatively connected to the first transmitter 302, the first optoelectronic module 304, the second optoelectronic module 308, the first receiver 314, the second transmitter 316, the third optoelectronic module 322, the fourth optoelectronic module 326, the second receiver 328, and the optional optoelectronic module 340 via communication links 330, 334, 336, 338, 344, 348, 350, 352, and 342, respectively.

In one embodiment, the abnormality detection system may be used to detect abnormality in the optical path length and the optical attenuation of the quantum channel. To avoid affecting the QKD operation, the first optoelectronic module 304 may inject pulsed light with a wavelength that is different from the light carrying quantum information into the first quantum channel 306. A fraction of the light, for example 50%, may be tapped and detected in the second optoelectronic module 308 to measure the optical path length and the optical attenuation of the first quantum channel 306 from the pulse arrival times and the detected optical power, respectively. The remaining light, in this example 50%, may be directed by the WDM coupler 310 to the optical link 312 and passed through the optional fifth optoelectronic module 340. The light then enters the second quantum channel 324 via the second WDM coupler 318 and is detected at the fourth optoelectronic module 326 to measure the optical path length and the optical attenuation of the second quantum channel 324 from the detection timing and the detected optical power, respectively.

In some embodiments, the optional fifth optoelectronic module 340 may contain an active device such as an optical amplifier that amplifies the optical power of the light that passes through it, for example, with a 3 dB gain. In other embodiments, the optional fifth optoelectronic module 340 may include an optical coupler that taps a portion of the light for measuring light pulse arrival times and mean-photon number using a photon detector, when the second optoelectronic module 308 does not make such measurements. The measured mean-photon number may be used to obtain the optical attenuation of the first quantum channel 306. This may be compared with previously measured values and the detection count rate recorded by the receiver 314. An abnormality is detected when a significant discrepancy is found.

Although it is shown that the abnormality detection system includes five optoelectronic modules 304, 308, 340, 322, 326, fewer or more than five optoelectronic modules may be used in practice to detect different abnormalities.

Although it is shown an inter-link connection of two QKD links, multiple inter-link connections may be constructed to connect more than two QKD links in a larger network.

Next, several embodiments of abnormality detection tests are described in detail. It should be appreciated that apart from the described embodiments, numerous alternative embodiments may be conceivable.

Fig. 4 shows an embodiment 400 of a QKD link equipped with an abnormality detection system. The QKD link includes a transmitter 402 sending light pulses carrying quantum information to

a receiver 432 over a quantum channel 420. The service channel for key distillation is omitted from the figure. The abnormality detection system comprises four optoelectronic modules, 406, 418, 422, 426, and two computing systems, 438 and 448.

The first optoelectronic module 406 is placed at the output port 404 of the transmitter 402. The second optoelectronic module 418 is placed next to the first optoelectronic module 406 and may include a first optical modulator, which may be an intensity modulator, a phase modulator, a polarization modulator, a frequency modulator, etc. and associated electronics such as a modulator driver. The third optoelectronic module 422 is placed before the fourth optoelectronic module 426 and may include a second optical modulator, which is of the same type as the first optical modulator 418 and associated electronics such as a modulator driver. The fourth optoelectronic module 426 is placed before the input port 430 of the receiver 432.

Each computing system may contain one or more processors, or processing units, for data processing, one or more memory devices for data storage, electronics for timing synchronization, time delay generation, etc. The computing system 438 is communicatively connected to the transmitter 402 via a physical link 434. It is also communicatively connected to the optoelectronic modules 406 and 418 via physical links 436 and 442, respectively. The computing system 448 is communicatively connected to the receiver 432 via a physical link 450. It is also communicatively connected to the optoelectronic modules 422 and 426 via physical links 444 and 446, respectively.

Clock signals may be sent from the transmitter 402 to the computing system 438, which then provide the clock signals to the optoelectronic modules 406 and 418 via physical links 436 and 442, respectively. Similarly, clock signals may be sent from the receiver 432 to the computing system 448, which then provide the clock signals to the optoelectronic modules 422 and 426 via physical links 444 and 446, respectively. The clock signals may be used to synchronize the operations of the optoelectronic modules 418 and 422, for example, when applying changes to light pulses carrying quantum information. The clock signals may also be used by the optoelectronic modules 406 and 426 if they use gated photon detectors.

The computing systems 438 and 448 are communicatively connected via the link 440. In general, the link 440 is over a public network and therefore, it needs to be encrypted and authenticated. In some embodiments, the link 440 may be protected with QKD keys.

In some embodiments, there may be only one computing system communicatively connected with the QKD system and all the optoelectronic modules 406, 418, 422, 426 for collecting and

processing all the data associated with the abnormality detection test. Any of these links over a public network is encrypted and authenticated.

Abnormality detection tests may be performed with only the first optoelectronic module 406, with only the fourth optoelectronic module 426, and with both optoelectronic modules 406 and 426, in the absence of optoelectronic modules 418 and 422. These embodiments shall be described before a specific embodiment of an abnormality detection test that employs all four optoelectronic modules 406, 426, 418, and 422 is described.

In a first embodiment, the abnormality detection test may be performed with only the first optoelectronic module 406 placed immediately at the output port 404 of the transmitter 402. The length of optical fibre connecting the transmitter 402 and the first optoelectronic module 406 may be a few centimetres or a few metres within a secure environment to ensure that no attacker may launch an attack between the transmitter 402 and the first optoelectronic module 406. The first optoelectronic module 406 includes a light source 408 which may be a laser source that is suitably attenuated and modulated, a first optical coupler 410 that preferably has a variable coupling ratio, an optical delay line 412 of a suitable length, a second optical coupler 414 that may have a variable coupling ratio or a fixed coupling ratio, for example 50:50, and at least one photosensitive device, for example, a first photon detector 416. In addition, the first optoelectronic module 406 may have a shutter (not shown) that may be used to block light coming from the transmitter 402 during test. Inside the first optoelectronic module 406, there may be a time-tagging module (not shown) to register the timestamps of photon detection events from the first photon detector 416. Other electronics, such as laser drivers, etc., are omitted for brevity.

This embodiment of abnormality detection system may be used to detect abnormality in the mean photon number of the light output from the transmitter 402, which may be caused by a malfunctioning component in the transmitter. During an abnormality detection test, the coupling ratio of the optical coupler 414 may be adjusted such that small known percentage, for example 1%, of the light from the transmitter 402 is tapped and detected by the photon detector 416. It is also possible to use an optical coupler 414 with a fixed coupling ratio that removes 1% of the light from the output port 404. The photon detector 416 records the photon count rate and infers the mean photon number of the light coming from the transmitter 402. If the inferred mean photon number is higher than the system designated value, an abnormality is detected. If the detection efficiency of the photon detector is 10%, then the mean-photon number per light pulse may be calculated from R / 0.001 / F, where F is the repetition rate of the light pulses, and R is the total measured photon count rate minus the dark count rate of

the photon detectors. The recorded photon count rate may also be compared against the photon count rate recorded by the QKD system to detect changes to the optical attenuation level of the quantum channel. In this case, the computing system 438 or 448 may obtain the photon count rate data from the QKD system.

This embodiment of abnormality detection system may also be used to detect abnormality in the QKD system's response to a QBER increase. For example, a malfunctioning or corrupted QKD system may provide a key rate that is independent of the QBER, compromising security as a result. During an abnormality detection test, the light source 408 sends photons at the QKD operating wavelength into the quantum channel via the first optical coupler 410. The coupling ratio of the optical coupler 410 may be adjusted to a suitable ratio such as 1%. The addition of noise photons unrelated to the QKD process increases the QBER. If the QKD system maintains a key rate that is unrelated to the addition of noise photons, an abnormality is detected. A variation to this embodiment is to tap a percentage, for example 5%, of the light from the output of the transmitter 402 and reinject the tapped light into the quantum channel after a suitable delay 412. If an increase in QBER is not registered, an abnormality is detected.

In a second embodiment, the abnormality detection test may be performed with only the fourth optoelectronic module 426 placed immediately before the input port 430 of the receiver 432. The length of optical fibre connecting the fourth optoelectronic module 426 and the receiver 432 may be a few centimetres or a few metres within a secure environment to ensure that no attacker may launch an attack between the fourth optoelectronic module 426 and the receiver 432. The fourth optoelectronic module 426 includes a third optical coupler 424 with a variable coupling ratio and at least one photosensitive device, for example a second photon detector 428. Inside the fourth optoelectronic module 426, there may be a time-tagging module (not shown) to register the timestamps of photon detection events from the second photon detector 428. Other electronics are omitted for brevity.

This embodiment of abnormality detection system may be used to detect abnormality in the mean-photon number of the light coming from the quantum channel 420. During abnormality detection test, the coupling ratio of the variable optical coupler 424 is dynamically varied in a random way that is unpredictable to any attacker. The proportion of the light intensity removed from the quantum channel 420 thus varies in accordance with the coupling ratio. The mean photon number measured at the receiver 432 also varies correspondingly. For example, if during an abnormality detection test, the coupling ratio of the optical coupler is set to remove 10% of the light from the quantum channel, the mean-photon number measured at the receiver would be 10% less than the previously recorded value. In the presence of a detector blinding

attack, the mean-photon number measured by the optoelectronic module 426 and the receiver 432 would not demonstrate such a correspondence.

In some variations, there may be an optical filter placed between the optical coupler 424 and the detector 428 to limit the light wavelength to the operating wavelength of the QKD system. In other variations, one or more photodiodes may be used in the optoelectronic module 426 to detect intense light. In other variations, two or more photon detectors may be used in the optoelectronic module 426 to detect changes in photon statistics.

In a third embodiment, an abnormality detection test may be performed with both the first optoelectronic module 406 and the fourth optoelectronic module 426, in the absence of optoelectronic modules 418 and 422. This embodiment of abnormality detection system may be used to detect various abnormalities.

An example is abnormality in the total optical attenuation experienced by the light sent from the transmitter. During abnormality detection test, the light source 408 in optoelectronic module 406 injects additional photons with a known mean-photon number into the quantum channel 420. A percentage of these photons are tapped using the optical coupler 424 and detected by the photon detector 428 in the optoelectronic module 426. The additional photons may be injected in a series of randomly timed short durations, such that the effect on QBER is not significant. From the count rate measured by the photon detector 428 in the optoelectronic module 426, the optical attenuation level of the quantum channel 420 can be determined. An abnormality is detected if the optical attenuation level of the quantum channel 420 has increased but the count rate detected by the receiver 432 remains unchanged. This abnormality may be the result of an attack in which an attacker tampers with the quantum channel 420 and the receiver 432.

In a fourth embodiment, an abnormality detection test may be performed with all four optoelectronic modules 406, 418, 422, 426. An objective of the test is to detect a known-basis attack, in which an attacker who knows the encoding basis choices of the transmitter 402 but not the encoded bit values, performs an intercept-resend attack. For example, the attacker may be a malicious insider who inserted malicious code into the transmitter 402 during the manufacturing process to corrupt its basis selection function such that the encoding basis choice follows a deterministic or pseudo-random bit pattern that is known either entirely or partially to the attacker. After the QKD system has been deployed, the attacker may then perform an intercept-resend attack on the light carrying quantum information at any point on the quantum channel 420 without increasing the QBER since the basis selection by the

attacker can always be the correct basis, i.e., same as the basis selected by the transmitter 402.

During abnormality detection test, both the optoelectronic module 418 and the optoelectronic module 422 may apply a change to the light in the quantum channel 420. The change may be a random modulation performed using an intensity modulator, phase modulator, polarization modulator, frequency modulator, time-delay modulator, or some other type of modulator. For illustration purpose, consider a phase encoded QKD system where quantum information is encoded onto the phase of weak light pulses. In a known-basis attack, the attacker, knowing the basis choice, performs an intercept-resend attack on the light carrying phase encoded quantum information without increasing the QBER.

This attack may be detected during an abnormality detection test in which the first phase modulator of the optoelectronic module 418 applies a random phase shift on the light coming from the transmitter 402. This is because the attacker does not know the timing and magnitude of the phase shift applied to the light by the optoelectronic modules 418 and 422 and hence, basis selection by the attacker in a known-basis attack cannot be always correct and this would lead to an increased QBER and in turn a decreased key rate. The second phase modulator of the optoelectronic module 422 applies a negative phase shift having the exact magnitude of that applied by the first phase modulator of the optoelectronic module 418 just before the light enters the receiver 432. The total phase shift applied by the phase modulators of the two optoelectronic modules 418 and 422 is thus equal to zero. In the absence of a known-basis attack, the QBER is not affected by the random phase modulation applied by the phase modulators of the two optoelectronic modules 418 and 422. In the presence of a known-basis attack, the phase shift applied by the second phase modulator of the optoelectronic module 422 does not negate the disturbance created by the attack.

The pattern for the random phase modulation may be determined by various ways. For example, by a real-time, randomly generated bit sequence. Alternatively, the pattern may be randomly selected from a predetermined group of pseudo-random patterns. For illustration, consider a randomly generated bit sequence of 110101011000... By grouping the bits in sets of 4, it may be interpreted as a random sequence of numbers between 0 and 15. In this case, the bit sequence is read as 13, 5, 8, ...

The first phase modulator of the optoelectronic module 418 may apply a phase shift of $13\pi/16$ radians for the first timeslot, followed by applying a phase shift of $5\pi/16$ radians for the second timeslot, followed by applying a phase shift of $\pi/2$ radians for the third timeslot, and so on. On

the other hand, the same bit sequence or pattern may be interpreted as applying a phase shift of -13π/16 radians for the first timeslot, followed by applying a phase shift of -5π/16 radians for the second timeslot, followed by applying a phase shift of -π/2 radians for the third timeslot, and so on for the second phase modulator in the optoelectronic module 422.

In an embodiment, the two optoelectronic modules 418 and 422 use the same random bit sequence to determine the phase modulation to apply but interpret it differently as described above, such that the net phase shift experienced by the light in the quantum channel remains unchanged throughout despite having phase modulation applied by the two optoelectronic modules 418 and 422. The random bit sequence may be generated from a seed shared by the two optoelectronic modules 418 and 422. Alternatively, it may be generated by one of the optoelectronic modules 418 or 422 and sent to the other optoelectronic module 422 or 418. Alternatively, it may be generated by one of the computing systems 438 or 448 and sent to the two optoelectronic modules 418 and 422.

Let the timing to apply a phase shift on one light pulse at the optoelectronic module 418 be T. Then the timing to reverse the phase shift on the same light pulse at the optoelectronic module 422 may be calculated from $T + L \cdot n/c$ where L is the length of the optical fibre between the two optoelectronic modules 418 and 422, n is the refractive index of the optical fibre and c is the speed of light in vacuum.

After the test has ended, both optoelectronic modules 418 and 422 stop the phase modulation. At least one of the computing systems 438, 448 obtains the QBER and the key rate data recorded during the test from the QKD devices 402 and 432 and processes the data. Under normal operating conditions and in the absence of a known-basis attack, neither the QBER nor the key rate should be affected by the test. If it is found that the QBER increased noticeably during the test leading to a decrease in key rate, it may be concluded that an abnormality has been detected.

It may be advantageous for the two optoelectronic modules 418 and 422 to apply the phase modulation in randomly timed short durations, for example of 1 ms duration each, instead of a long continuous duration. This is to prevent a noticeable change to the QBER during test in the presence of an attack since a compromised receiver may monitor the QBER and revert to normal behaviour whenever it detects a slightly increased QBER. After the test has completed, at least one computing system in 438, 448 obtains raw data from the QKD system corresponding to the time range that covers the short durations. It is then possible for the computing system 438, 448 to aggregate the raw data recorded during the bursts of short test

durations when a random phase shift was applied by the optoelectronic modules 418 and 422 to obtain the overall QBER during test. Since a compromised QKD system cannot know when the short durations of phase modulation occurred, it will not detect a noticeable change to the QBER during test in the presence of a known-basis attack.

A compromised transmitter 402 may send more intense light pulses into the second optoelectronic module 418 such that an attacker through measuring the more intense light pulses that passed through the first optoelectronic module 418 may learn the phase modulation. The role of the first optoelectronic module 406 is to detect such more intense light pulses coming from the transmitter 402. To prevent the transmitter from blinding the first photon detector, an additional photodiode may be used in the first optoelectronic module 406 to detect intense light. The first optoelectronic module 406 may also be used to detect a higher mean-photon number coming from the transmitter 402, which could be due to system malfunction.

An attacker may launch a Trojan horse attack by sending more intense light pulses from the quantum channel 420 into the optoelectronic module 422 and attempt to capture a reflection from the optoelectronic module 426 or the receiver 432 to learn the modulation applied by the optoelectronic module 422. The role of the fourth optoelectronic module 426 is to detect such more intense pulses coming from the quantum channel. The fourth optoelectronic module 426 may also be used to detect a discrepancy in the photon detection rate recorded by the fourth optoelectronic module 426 and the receiver 432, which is an abnormality that could be due to a detector blinding attack. At least one external optical isolator may further be included in the fourth optoelectronic module 426, preferably between the optoelectronic module 422 and the optical coupler 424, to suppress any reflected light or light escaping from the receiver 432.

An attacker may also launch a Trojan horse attack by sending more intense light pulses from the quantum channel 420 into the optoelectronic module 418 and attempt to capture a reflection that carries information on the modulation applied by the optoelectronic module 418. At least one external optical isolator may be placed immediately before the output port of the optoelectronic module 418 to block any such attack.

It is envisaged that any kind of optical modulation may be used with the disclosed method. For example, polarization modulation may be used with polarization encoded QKD. In this case, the optoelectronic module 418 applies a random polarization modulation, which is reversed by the optoelectronic module 422. The random polarization modulation does not affect the QBER of the QKD link because it does not involve measuring the quantum information.

Time-delay modulation may also be used to detect a known basis attack. This method is independent of the type of encoding of quantum information and may be used with QKD protocols based on polarization encoding, time-bin encoding, phase-encoding, etc. An attacker who cannot predict when a time-delay modulation is applied cannot perform a known-basis attack at the right timing even though the attacker may have knowledge of the basis choices made by the transmitter.

Fig. 5 shows an embodiment 500 of a QKD link equipped with an abnormality detection system based on time-delay modulation for detecting the known-basis attack. A transmitter 502 sends light pulses carrying quantum information to a receiver 576 over a quantum channel 540. The transmitter 502 and the receiver 576 perform key distillation over a service channel (not shown). The abnormality detection system comprises a first optoelectronic module 506, a second optoelectronic module 544, a first computing system 538, and a second computing system 572. The first computing system 538 is communicatively connected to the first optoelectronic module 506 via a communication link 532 and to the transmitter 502 via another communication link 536. The second computing system 572 is communicatively connected to the second optoelectronic module 544 via a communication link 570 and to the receiver 576 via another communication link 580. The two computing systems 538 and 572 are communicatively connected to each other via communication link 542. The first optoelectronic module 506 receives clock signals from the transmitter 502 via a physical link 530, while the second optoelectronic module 544 receives clock signals from the receiver 576 via another physical link 578.

The optoelectronic modules 506 and 544 are identical. Therefore, only the optoelectronic module 506 is described below. It includes a first 1x4 optical switch 508 with an input port 504, a second 1x4 optical switch 514 with an output port 540, a first optical link 524, a second optical link 520 with an optical delay line 522, a third optical link 516 with an optical delay line 518, a fourth optical link 510 with an optical delay 512, a controller unit 534, a first physical connection 526 between the first optical switch 508 and the controller unit 534, and a second physical connection 528 between the second optical switch 514 and the controller unit 534.

During operation, the first 1x4 optical switch 508 takes in light from its input port 504 and switches the light to one of its four output optical links, 524, 520, 516 or 510. The second 1x4 optical switch 514 takes in light from either one of its four input optical links 524, 520, 516 or 510 and switches the light to its output port, which is connected to the quantum channel 540. The lengths of the optical delay lines 522, 518, 512 are determined by the required amount of

time delay to apply to the light for one-period, two-period, or three-period delays, respectively. For example, if the input light includes light pulses separated by period T [s], then the length L [m] of the optical delay line 522 to delay the time of the light by one period is obtained from T * c / n, where c = 2.998 x 108 m/s is the speed of light and n is the refractive index of the optical delay line. A typical value for the refractive index is n = 1.47. For example, if T = 100 ns, L = 20.4 m for one-period delay.

The controller unit 534 takes in clock signals from the transmitter 502 via the physical link 530 so that it may synchronize the switching time with the arrival time of the light pulses. The controller unit 534 may include electronic subsystems such as phase-locked loops, delay generators, etc., for timing synchronization. The controller unit 534 sends electrical signals synchronized to the received clock signals to the two optical switches 508 and 514 such that they operate in tandem. When the first optical switch 508 directs light from the transmitter output 504 to the first optical link 524, the second optical switch 514 directs the light from the first optical link 524 to the quantum channel 540. When the first optical switch 508 directs light from the transmitter output 504 to the second optical link 520 with optical delay line 522, the second optical switch 514 directs the light from the second optical link 520 with optical delay line 522 to the quantum channel 540, and so on. The controller unit 534 may receive instructions from or send data to the computing system 538 via the communication link 532. In some variations, the controller unit 534 and the computing system 538 may be integrated together.

In one embodiment, under normal operating conditions, light entering the first optoelectronic module 506 passes through the optical link 510 with the longest optical delay line 512, while light entering the second optoelectronic module 544 passes through the optical link 562 without optical delay line. Let the overall optical path length in this case be denoted by L. During an abnormality test, for a randomly selected duration, the two optical switches, 508 and 514, of the first optoelectronic module 506 switches the light such that it passes through an optical link randomly selected from 524, 520, 516, 510, while the two optical switches, 546 and 552, of the second optoelectronic module 544 switch the light such that it passes through a corresponding optical link selected from 562, 558, 554, 548 such that the overall optical path length L is maintained. For example, if the randomly selected optical link in the first optoelectronic module 506 is the optical link 520 with the optical delay line 522, then the selected corresponding optical link in the second optoelectronic module 544 is the optical link 554 with the optical delay line 556.

The pattern for the random switching may be determined by a real-time, randomly generated bit sequence. Alternatively, the pattern may be randomly selected from a predetermined group of pseudo-random patterns. For simple illustration, consider an embodiment in which the number of delays choices N = 2. A randomly generated bit sequence or pattern of 111001000... may be interpreted as switching to the longer optical link for 3 timeslots, followed by the shorter optical link for 2 timeslots, followed by the longer optical link for 1 timeslot, followed by the shorter optical link for 3 timeslots, and so on for the first optoelectronic module 506. On the other hand, the same bit sequence or pattern may be interpreted as switching to the shorter optical link for 3 timeslots, followed by the longer optical link for 2 timeslots, followed by the shorter optical link for 1 timeslot, followed by the longer optical link for 3 timeslots, and so on for the second optoelectronic module 544. It should be noted that the two optoelectronic modules 506 and 544 use the same random pattern but interpret it differently, such that the total optical path length L traversed by the light in the quantum channel remains unchanged despite the switching. For N = 4, two bits may be used to randomly select one out of the four optical links. In this case, the random bit consumption rate is twice as fast.

After the test has ended, the optical switches in both optoelectronic modules 506 and 544 revert to their original states. At least one of the computing systems 538, 572 obtains the QBER and the key rate data recorded during the test from the QKD devices (i.e. the transmitter 502 and the receiver 576) and processes the data. If found that the QBER increased during the test, it may be concluded that an abnormality has been detected.

Although there is active random optical switching of optical links having different optical delay lengths inside the two optoelectronic modules 506 and 544 during the abnormality detection test, to the QKD link, the total path length L of the quantum channel remains unchanged throughout. There should not be any change to the arrival timing of the light carrying quantum information at the receiver 576. Neither the QBER nor the key rate should be affected by the test. In the event where there is an ongoing known-basis attack, since the attacker does not have knowledge of the time delay modulation, an intercept-resend attack performed at any point on the quantum channel will certainly cause the QBER to increase and the key rate to decrease. In this way, the attack can be detected.

In practice, a large N is preferred as the probability of N consecutive basis choices being the same will be smaller. If N = 2, an attacker launching a known basis attack may learn more than 1/4 of the bits without causing errors as the attacker may choose to eavesdrop only when two or more consecutive basis choices are the same such that the attack is not detectable by

the test method described above. For a larger N, the number of bits that can be eavesdropped without causing errors may be significantly reduced.

Whenever a switch of delay line is performed, an error may occur at the timing of the switch because the light pulses at the output of the time-delay modulator collide due to a delayed light pulse overlapping with a later light pulse. If the switching of delay line does not occur often, the increase in QBER due to this effect may be negligible.

It should be appreciated that optoelectronic modules 506 and 544 correspond to optoelectronic modules 418 and 422 of Fig. 4, respectively, and the optoelectronic modules 406 and 426 may be included herein for the same reasons as described above.

Fig. 6 shows the concept 600 of randomly timed short durations. The first row of bit values 602 is an example of bit-value encoding at a transmitter. The shaded boxes 604, 606, 608, 610 are randomly timed short durations in which a modulation is applied to the light pulses in the quantum channel. The second row of bit values 612 is an example of detected bit values at a receiver. Empty boxes denote photons lost during transmission. The total number of errors is 3 out of 17 for the detected bits in this example. The QKD system does not know the randomly timed short durations. Therefore, it may only calculate the overall error rate.

Only the abnormality detection system who knows the randomly timed short durations may calculate the aggregated error rate during the applied modulation. The number of errors is 3 out of 5 for the detected bits that correspond to light pulses that experienced the change applied by the time-delay modulator. In this example, the error rate for the detected bit values falling within the randomly timed short durations is much higher than normal. An abnormality may be detected in this way. In practice, a threshold may be set by the abnormality detection system. This method prevents a compromised QKD system from detecting a noticeable increase in the QBER such that it cannot evade detection.

To perform the QBER calculation, the abnormality detection system obtains raw bit values from the QKD system. The request for raw data should not give information about the time and duration of the test. Preferably, the raw key bits collected during the test shall be discarded, such that they do not contribute to the generation of the final secret key.

It is advantageous for an abnormality detection test in which an increase in QBER during test indicates the presence of an abnormality be interleaved with randomly timed short durations in which noise photons are injected into the quantum channel to deliberately increase the

QBER. If found that the QBER does not increase during those durations in which noise photons are injected, an abnormality is detected.

It is also advantageous that different abnormality detection tests may be combined and placed into one optoelectronic module and an optoelectronic module may be configured in any number of different ways to perform a variety of abnormality detection tests, either sequentially or simultaneously.

It is further advantageous to combine the abnormality detection testing methods disclosed herein with other methods of QKD system integrity check or tamper detection, for example, the method described in PCT/SG2022/050865, which is incorporated herein by reference.

It should be noted that although a discrete-variable prepare-and-measure QKD protocol has been assumed in several of the embodiments, the systems and methods described herein are also applicable to various types of QKD protocols, such as continuous-variable QKD, measurement-device-independent QKD, etc.

Whilst the foregoing description has described exemplary embodiments, it will be understood by those skilled in the art that many variations of the embodiments can be made.

CLAIMS

1. A method for detecting abnormality in a quantum key distribution (QKD) system, the method comprising:

applying a change to light in a quantum channel of the QKD system, wherein one or more characteristics of the change are not made known to one or more components of the QKD system before or during applying the change;

collecting or receiving data associated with the applied change;

obtaining a value of a property of the QKD system using the collected or received data;

comparing the obtained value to an expected value of the property of the QKD system; and

identifying a discrepancy or deviation in the obtained value, wherein the discrepancy or deviation indicates abnormality in the QKD system.

2. The method of claim 1, wherein the one or more characteristics of the change comprise the type of the change, the time of applying the change, the duration of applying the change, the magnitude of the change, and/or the pattern of the change, and/or

wherein, at least one of the one or more characteristics of the change is determined randomly or intentionally made unpredictable to any attacker, and/or

wherein, the change comprises one or more of the following:

- removing an amount of light from the quantum channel,
- adding an amount of light into the quantum channel,
- modulating a property of the light in the quantum channel, the property of the light comprising one or more of the optical properties of the light, including optical intensity, phase, time delay, wavelength, frequency, or polarization of the light, and/or

wherein, the change is applied for short durations, preferably randomly timed, to avoid noticeably affecting the operation of the QKD system, and/or

wherein, the received data includes one or more of encoding basis choices, bit-value choices, decoding basis choices, detection timestamps, and/or detected bit values, and raw key bits associated with the received data are preferably not used by the QKD system for secret key generation, and/or

wherein, the expected value of the property of the QKD system comprises one or more of an estimated, modelled, or simulated value, or a range of values, or past obtained values of the same property, and/or

wherein, the property of the QKD system comprises one or more of the following:

- a mean photon number of the light sent from a transmitter;

- a total optical attenuation experienced by the light in the quantum channel;
- a total optical path length traversed by the light in the quantum channel;
- an amount of noise in the quantum channel,
- a quantum bit-error rate (QBER), or
- a key rate.

3. The method of claim 1, further comprising providing one or more characteristics of the change via at least one processing unit to one or more optoelectronic modules applying the change, wherein the at least one processing unit is in the one or more optoelectronic modules or in a computing system preferably operating independently from the QKD system.

4. The method of claim 2, wherein the change is applied for short durations to avoid noticeably affecting the operation of the QKD system, the method further comprising providing a time and duration associated with the short durations to the QKD system after applying the change.

5. The method of claim 3, further comprising the steps of:

applying a first modulation to a property of the light in the quantum channel of the QKD system, the first modulation applied via a first optoelectronic module of the one or more optoelectronic modules; and

applying a second modulation to a property of the light in the quantum channel of the QKD system, the second modulation applied via a second optoelectronic module of the one or more optoelectronic modules, wherein the second modulation is configured to reverse or cancel the first modulation, and

obtaining the QBER during the application of the first modulation and the second modulation, wherein an increase in the QBER provides a detection of abnormality.

6. The method of claim 3, further comprising:

removing a proportion of light from the quantum channel via an optoelectronic module of the one or more optoelectronic modules preferably located near a transmitter of the QKD system, optionally wherein the proportion of light removed is 1%,

measuring a mean photon number of the removed light, and

identifying a deviation in the mean photon number value from an expected value or range of values or past obtained values, wherein the deviation indicates abnormality in the QKD system.

7 The method of claim 3, further comprising:

applying an intensity modulation to the light in the quantum channel of the QKD system via an optoelectronic module of the one or more optoelectronic modules preferably placed near a receiver of the QKD system, preferably wherein the intensity modulation is randomly determined or intentionally made unpredictable to any attacker; and

measuring if a count rate deviates from an expected value or range of values or past obtained values, wherein a deviation indicates abnormality in the QKD system.

8. The method of claim 3, further comprising

adding an amount of light into the quantum channel of the QKD system;

removing an amount of light from the quantum channel of the QKD system;

measuring a photon arrival time and mean photon number of the removed light, and

processing the measured data to obtain the optical path length traversed by the light in the quantum channel and the optical attenuation experienced by the light in the quantum channel, wherein a deviation from an expected value or range of values or past obtained values indicates abnormality in the QKD system.

9. The method of claim 3, further comprising:

performing an emulated eavesdropping to increase the QBER of the QKD system for one or more time durations, wherein the one or more time durations are preferably not made known to the QKD system before or during performing the emulated eavesdropping;

obtaining from the QKD system data taken during the one or more time durations; and

processing the obtained data to determine if the QBER increased during the one or more time durations, wherein the absence of an increase in the QBER indicates abnormality in the QKD system.

10. A method for detecting abnormality in a quantum key distribution (QKD) system, wherein one or more of the methods according to claims 5, 6, 7, 8, 9 are implemented individually, in parallel, in series, or in any combination.

11. A system for detecting abnormality in a QKD system, the system comprising:

one or more optoelectronic modules configured to apply a change to light in a quantum channel of the QKD system, wherein one or more characteristics of the change are not made known to of the QKD system before or during applying the change, and

at least one processing unit configured to:

collect or receive data associated with the applied change;

obtain a value of a property of the QKD system using the collected or received data;

compare the obtained value to an expected value of the property of the QKD system; and

identify a discrepancy or deviation in the obtained value, wherein the discrepancy or deviation indicates abnormality in the QKD system.

12. The system of claim 11, wherein the one or more characteristics of the applied change comprise the type of the change, the time of applying the change, the duration of applying the change, the magnitude of the change, and/or the pattern of the change, and/or

wherein, at least one of the one or more characteristics of the change is determined randomly or intentionally made unpredictable to any attacker, and/or

wherein, the change comprises one or more of the following:

- removing an amount of light from the quantum channel,
- adding an amount of light into the quantum channel,
- modulating a property of the light in the quantum channel, the property of the light comprising one or more of the optical properties of the light, including optical intensity, phase, time delay, wavelength, frequency, or polarization of the light, and/or

wherein, the change is applied for short durations, preferably randomly timed, to avoid noticeably affecting the operation of the QKD system, and/or

wherein, the received data includes one or more of encoding basis choices, bit-value choices, decoding basis choices, detection timestamps, and/or detected bit values, and/or

wherein one or more raw key bits associated with the received data are preferably not used by the QKD system for secret key generation, and/or

wherein, the expected value of the property of the QKD system comprises one or more of an estimated, modelled, or simulated value, or a range of values, or past obtained values of the same property, and/or

wherein, the property of the QKD system comprises one or more of the following:

- a mean photon number of the light sent from a transmitter;
- a total optical attenuation experienced by the light in the quantum channel;
- a total optical path length traversed by the light in the quantum channel;
- an amount of noise in the quantum channel,
- a quantum bit-error rate (QBER), or
- a key rate.

13. The system of claim 11, wherein the at least one processing unit is configured to provide the one or more characteristics of the change to the one or more optoelectronic modules applying the change, and wherein the at least one processing unit is in the one or

more optoelectronic modules or in a computing system preferably operating independently from the QKD system.

14. The system of claim 12, wherein the change is applied for short durations to avoid noticeably affecting the operation of the QKD system, the at least one processing unit is configured to provide a time and duration associated with the short durations to the QKD system after applying the change.

15. The system of claim 11, wherein the one or more optoelectronic modules comprise:

a first optoelectronic module, preferably located near a transmitter of the QKD system, configured to apply a first modulation to apply a first modulation to a property of the light in the quantum channel of the QKD system,

a second optoelectronic module, preferably located near a receiver of the QKD system, configured to apply a second modulation to a property of the light in the quantum channel of the QKD system, wherein the second modulation is configured to reverse or cancel the first modulation, and

wherein the at least one processing unit is configured to obtain the QBER during the application of the first modulation and the second modulation, and wherein an increase in the QBER provides a detection of abnormality.

16. The system of claim 11, wherein the one or more optoelectronic modules comprise at least one optoelectronic module, preferably located near a transmitter of the QKD system, the at least one optoelectronic module being configured to:

remove a proportion of light from the quantum channel, optionally wherein the proportion of light removed is 1%

measure the mean photon number of the removed light, and

at least one processing unit, configured to:

identify a deviation in the mean photon number value from an expected value or range of values or past obtained values, wherein the deviation indicates abnormality in the QKD system.

17. The system of claim 11, wherein one of the one or more optoelectronic modules is configured to apply an intensity modulation to the light in the quantum channel of the QKD system via an optoelectronic module preferably placed near the receiver of the QKD system, preferably the intensity modulation is randomly determined or intentionally made unpredictable to any attacker; and

wherein the at least one processing unit is configured to measure if a count rate deviates from an expected value or range of values or past obtained values, wherein a deviation indicates abnormality in the QKD system.

18. The system of claim 11, wherein the one or more optoelectronic modules are configured to:

add an amount of light into the quantum channel of the QKD system,

remove an amount of light from the quantum channel of the QKD system,

measure a photon arrival time and mean photon number of the removed light, and

wherein the at least one processing unit is configured to process the measured data to obtain the optical path length traversed by light in the quantum channel and the optical attenuation experienced by light in the quantum channel, wherein a deviation from an expected value or range of values or past obtained values indicates an abnormality in the QKD system.

19. The system of claim 11, wherein the one or more optoelectronic modules are configured to:

perform an emulated eavesdropping to increase the QBER of the QKD system for one or more time durations, wherein the one or more time durations are preferably not made known to the QKD system before or during the performing of the emulated eavesdropping, and

wherein the at least one processing unit is configured to

obtain from the QKD system data taken during the one or more time durations;

process the obtained data to determine if the QBER increased during the one or more time durations, wherein the absence of an increase in the QBER indicates abnormality in the QKD system.

20. A system for detecting abnormality in a QKD system, wherein any number of optoelectronic modules and processing units according to claims 15, 16, 17, 18, 19 are configured to operate individually, in parallel, in series, or in any combination.