

payment transactions or banking activities on the World Wide Web. In a conventional HTTPS setting, before data transmission, the server side and client side agree on an encryption scheme and keys that will be used to exchange data. The client may generate a pre-master key, encrypt the pre-master key using the server's public key, and send the encrypted pre-master key to the server. Both the server and client can then generate a master key (also known as the session key) based on the pre-master key. The session key can then be used to encrypt data flows between the client and server.

[0004] Although current secure data transmission technologies, including HTTPS, can provide certain protections against common attacks, such as simple man-in-the-middle attacks and eavesdropping attacks, they may still be vulnerable to other types of attacks. For example, HTTPS can be vulnerable to more sophisticated man-in-the-middle attacks and a range of traffic analysis attacks. Moreover, the advance in computational capabilities provided by cloud computing and quantum computing has increased the possibility of successful brute-force attacks. For example, an attacker may obtain the public-key-encrypted master key via eavesdropping and launch a brute-force attack to obtain the master key. As a result, any subsequent data communication using that master key will be compromised.

[0005] Moreover, current secure data transmission technologies often rely on hash-based techniques to detect eavesdropping attacks. Although these hash-based techniques can be used to verify data integrity, they often cannot detect passive eavesdropping, where attackers can copy or perform measurements on the transmitted signals.

SUMMARY

[0005a] Aspects of the invention are defined in the independent claims. Some optional features of the invention are defined in the dependent claims.

[0006] One exemplary technique provides a system and method for detecting eavesdropping while establishing secure communication between a local node and a remote node. During operation, the local node generates a random key and a regular optical signal based on the random key. The local node also generates a quantum optical signal based on a control sequence and a set of quantum state bases, and multiplexes the regular optical signal and the quantum optical signal to produce a hybrid optical signal. The local node transmits the hybrid optical signal to the remote node, sends information associated with the control sequence

and information associated with the set of quantum state bases to the remote node, and receives an eavesdropping-detection result from the remote node based on measurement of the quantum optical signal, the information associated with the control sequence, and the information associated with the set of quantum state bases.

5 **[0007]** In a variation, the local node encrypts the random key.

[0008] In a variation, generating the quantum optical signal comprises: generating a random binary string as the control sequence; selecting, from a quantum-state-basis library, the set of quantum state bases; assigning a length value for each selected quantum state basis; and encoding a number of single photons based on the control sequence, the set of quantum state
10 bases, and the length values assigned to the quantum state bases. A sum of length values of the selected quantum state bases equals a length of the control sequence.

[0009] In a further variation, encoding the single photons comprises: associating a bit in the control sequence with a quantum state basis within the selected set of quantum state bases based on a position of the bit and assigned lengths of the selected set of quantum state bases, and
15 modulating a polarization state of a single photon based on a value of the bit and the associated quantum state basis.

[0010] In a variation, the information associated with the control sequence includes a length of the control sequence and bit values of the control sequence. The information associated with the set of quantum state bases comprises quantum-state-basis identifiers (QIDs)
20 of the set of quantum state bases and length values corresponding to the QIDs.

[0011] In a variation, in response to the eavesdropping-detection result indicating that no eavesdropping is detected, the system establishes a secure communication channel between the first and second nodes using the random key.

[0012] One exemplary technique described herein provides a system and method for
25 detecting eavesdropping while establishing secure communication between a local node and a remote node. During operation, the local node receives from the remote node a hybrid optical signal comprising a regular optical signal multiplexed with a quantum optical signal. The regular optical signal carries information associated with a random key, and the quantum optical signal is generated based on a control sequence and a first set of quantum state basis. The local
30 node demultiplexes the received hybrid optical signal to obtain the regular optical signal and the quantum optical signal, processes the regular optical signal to obtain the random key, and

performs measurement on the quantum optical signal using a second set of quantum state bases. The local node receives from the remote node information associated with the control sequence and information associated with the first set of quantum state bases and generates an eavesdropping-detection result based on the measurement of the quantum optical signal, the
5 information associated with the control sequence, and the information associated with the first set of quantum state bases.

[0013] One exemplary technique described herein provides a system and method for detecting eavesdropping while establishing secure communication between a local node and a remote node. During operation, the local node generates a regular optical signal based on data to
10 be transmitted, generates a quantum optical signal based on a control sequence and a set of quantum state bases, and multiplexes the regular optical signal and the quantum optical signal to produce a hybrid optical signal. The local node then transmits the hybrid optical signal to the remote node and sends information associated with the control sequence and information associated with the set of quantum state bases to the remote node. The local node receives an
15 eavesdropping-detection result from the remote node based on measurement of the quantum optical signal, the information associated with the control sequence, and the information associated with the set of quantum state bases.

BRIEF DESCRIPTION OF THE FIGURES

20 [0013a] Embodiments of the invention will now be described, by way of example only, and with reference to the accompanying drawings in which:

[0014] FIG. 1 illustrates a time-state diagram describing the process of establishing a conventional HTTPS channel.

[0015] FIG. 2 presents a time-state diagram describing the process of establishing a
25 quantum-enhanced HTTPS channel, according to one embodiment of the present invention.

[0016] FIG. 3 presents a diagram illustrating an exemplary client device, in accordance with one embodiment of the present invention.

[0017] FIG. 4 presents a diagram illustrating an exemplary server device, in accordance with one embodiment of the present invention.

[0018] FIG. 5 illustrates an exemplary client-server network environment for implementing the disclosed eavesdropping-detection technology, in accordance with some embodiments described herein.

5 [0019] FIG. 6 conceptually illustrates an electronic system with which some implementations of the subject technology are implemented.

[0020] Table 1 illustrates two exemplary mechanical quantity measurement schemes based on using two different sets of quantum states in accordance with one embodiment described herein.

10 [0021] In the figures, like reference numerals refer to the same figure elements.

DETAILED DESCRIPTION

[0022] The following description is presented to enable any person skilled in the art to make and use the embodiments, and is provided in the context of a particular application and its requirements. Various modifications to the disclosed embodiments will be readily apparent to those skilled in the art, and the general principles defined herein may be applied to other

15

What Is Claimed Is:

1. A method for detecting eavesdropping while establishing secure communication between a local node and a remote node, the method comprising:
 - 5 generating, by the local node, a random key;
generating a regular optical signal based on the random key;
generating a quantum optical signal based on a control sequence and a plurality of quantum state bases, wherein the control sequence comprises a random binary bit string, and each quantum state basis includes orthogonal quantum states, wherein the
 - 10 generating comprises:
 - encoding each bit of the control sequence using a randomly selected quantum state basis of the plurality of quantum state bases;
multiplexing the regular optical signal and the quantum optical signal to produce a hybrid optical signal;
 - 15 transmitting the hybrid optical signal to the remote node;
sending information associated with the control sequence and information associated with the plurality of quantum state bases to the remote node; and
receiving an eavesdropping-detection result from the remote node based on measurement of the quantum optical signal, the information associated with the
 - 20 control sequence, and the information associated with the plurality of quantum state bases.
2. The method of claim 1, further comprising encrypting, by the local node, the random key.
- 25 3. The method of claim 1, wherein generating the quantum optical signal comprises:
 - generating the random binary string as the control sequence;
selecting, from a quantum-state-basis library, the plurality of quantum state
 - 30 bases;

assigning a length value for each selected quantum state basis, wherein a sum of length values of the selected quantum state bases equals a length of the control sequence; and

5 encoding a number of single photons based on the control sequence, the plurality of quantum state bases, and the length values assigned to the quantum state bases.

4. The method of claim 3, wherein encoding the single photons comprises:
associating a bit in the control sequence with the randomly selected quantum
10 state basis of the selected plurality of quantum state bases based on a position of the bit and assigned lengths of the selected plurality of quantum state bases; and
modulating a polarization state of a single photon based on a value of the bit encoded with the associated quantum state basis.

15 5. The method of claim 1, wherein the information associated with the control sequence comprises a length of the control sequence and bit values of the control sequence, and wherein the information associated with the plurality of quantum state bases comprises quantum-state-basis identifiers (QIDs) of the plurality of quantum state bases and length values corresponding to the QIDs.

20

6. The method of claim 1, further comprising:
in response to the eavesdropping-detection result indicating that no
eavesdropping is detected, establishing a secure communication channel between the
local and remote nodes using the random key.

25

7. A local system for detecting eavesdropping while establishing secure communication between the local system and a remote system, the local system comprising:

a quantum-state-basis library of quantum state bases, wherein each quantum
30 state basis includes orthogonal quantum states;

a random-key generator configured to generate a random key;

a regular optical module configured to generate a regular optical signal based on the random key;

a quantum optical encoder configured to generate a quantum optical signal based on a control sequence and a plurality of quantum state bases selected from the quantum-state-basis library, wherein the control sequence comprises a random binary bit string, the quantum optical encoder is configured to generate the quantum optical signal by encoding each bit of the control sequence using a randomly selected quantum state basis of the plurality of quantum state bases; and

an optical multiplexer configured to multiplex the regular optical signal and the quantum optical signal to produce a hybrid optical signal to be transmitted to the server;

wherein the regular optical module is further configured to:

send information associated with the control sequence and information associated with the plurality of quantum state bases to the remote system; and

receive an eavesdropping-detection result from the remote system based on measurement of the quantum optical signal, the information associated with the control sequence, and the information associated with the plurality of quantum state bases.

8. The local system of claim 7, wherein while generating the quantum optical signal, the quantum optical encoder is configured to:

generate a random binary string as the control sequence;

select, from the quantum-state-basis library, the plurality of quantum state bases;

assign a length value for each selected quantum state basis, wherein a sum of length values of the selected quantum state bases equals a length of the control sequence; and

encode a number of single photons based on the control sequence, the plurality of quantum state bases, and the length values assigned to the quantum state bases.

9. The local system of claim 8, wherein while encoding the single photons, the quantum optical encoder is configured to:

associate a bit in the control sequence with the randomly selected quantum state basis of the selected plurality of quantum state bases based on a position of the bit and assigned lengths of the selected plurality of quantum state bases; and

5 modulate a polarization state of a single photon based on a value of the bit encoded with the associated quantum state basis.

10. The local system of claim 7, wherein the information associated with the control sequence comprises a length of the control sequence and bit values of the control sequence, and wherein the information associated with the plurality of
10 quantum state bases comprises quantum-state-basis identifiers (QIDs) of the plurality of quantum state bases and length values corresponding to the QIDs.

11. A method for detecting eavesdropping while establishing secure communication between a local node and a remote node, the method comprising:
15 receiving, by the local node from the remote node, a hybrid optical signal comprising a regular optical signal multiplexed with a quantum optical signal, wherein the regular optical signal carries information associated with a random key, and wherein the quantum optical signal is generated based on a control sequence and a first plurality of quantum state bases, each quantum state basis including orthogonal
20 quantum states, wherein the control sequence comprises a random binary bit string and the quantum optical signal is generated by encoding each bit of the control sequence using a randomly selected quantum state basis of the first plurality of quantum state bases;

demultiplexing the received hybrid optical signal to obtain the regular optical
25 signal and the quantum optical signal;

processing the regular optical signal to obtain the random key;

performing measurement on the quantum optical signal using a second plurality of quantum state bases;

receiving, from the remote node, information associated with the control
30 sequence and information associated with the first plurality of quantum state bases;
and

generating an eavesdropping-detection result based on the measurement of the quantum optical signal, the information associated with the control sequence, and the information associated with the first plurality of quantum state bases.

- 5 12. The method of claim 11, wherein the information associated with the control sequence comprises a length of the control sequence and bit values of the control sequence, and wherein the information associated with the first plurality of quantum state bases comprises quantum-state-basis identifiers (QIDs) of the plurality of quantum state bases and length values corresponding to the QIDs.
- 10 13. The method of claim 12, wherein generating the eavesdropping-detection result comprises:
- calculating a photon loss rate based on the measurement of the quantum optical signal and the length of the control sequence; and
- 15 in response to determining that the photon loss rate is less than a predetermined threshold, generating an eavesdropping-detection result indicating that no eavesdropping is detected.
14. The method of claim 12, wherein generating the eavesdropping-detection result involves:
- 20 calculating a bit error rate based on the measurement of the quantum optical signal, the bit values of the control sequence, the QIDs of the first plurality of quantum state bases, the length values corresponding to the QIDs, and the second plurality of quantum state bases; and
- 25 in response to determining that the bit error rate is less than a predetermined threshold, generating an eavesdropping-detection result indicating that no eavesdropping is detected.
15. The method of claim 11, further comprising:
- 30 in response to the eavesdropping-detection result indicating that no eavesdropping is detected, establishing a secure communication channel between the local and remote nodes using the random key.

16. A local system for detecting eavesdropping while establishing secure communication between the local system and a remote system, the local system comprising:

5 a quantum-state-basis library of quantum state bases, wherein each quantum state basis includes orthogonal quantum states;

an optical demultiplexer configured to demultiplex a hybrid optical signal received from the remote system to obtain a regular optical signal and a quantum optical signal, wherein the regular optical signal carries information associated with a random key, and wherein the quantum optical signal is generated based on a control sequence and a first plurality of quantum state bases, wherein the control sequence comprises a random binary bit string and the quantum optical signal is generated by encoding each bit of the control sequence using a randomly selected quantum state basis of the first plurality of quantum state bases;

10

15 a regular optical module configured to receive and process the regular optical signal to obtain the random key;

a quantum-state-measurement module configured to perform measurement on the quantum optical signal using a second plurality of quantum state bases; and

an eavesdropping-detection-result generator configured to:

20 receive, from the remote system via the regular optical module, information associated with the control sequence and information associated with the first plurality of quantum state bases; and

generate the eavesdropping-detection result based on the measurement of the quantum optical signal, the information associated with the control sequence, and the information associated with the first plurality of quantum state bases.

25

17. The local system of claim 16, further comprising an encryption/decryption module configured to decrypt the regular optical signal to obtain the random key.

30

18. The local system of claim 16, wherein the information associated with the control sequence comprises a length of the control sequence and bit values of the

control sequence, and wherein the information associated with the first plurality of quantum state bases comprises quantum-state-basis identifiers (QIDs) of the plurality of quantum state bases and length values corresponding to the QIDs.

5 19. The local system of claim 18, wherein while generating the eavesdropping-detection result, the eavesdropping-detection-result generator is further configured to:
 calculate a photon loss rate based on the measurement of the quantum optical signal and the length of the control sequence; and
 in response to determining that the photon loss rate is less than a predetermined
10 threshold, generate an eavesdropping-detection result indicating that no eavesdropping is detected.

20. The local system of claim 18, wherein while generating the eavesdropping-detection result, the eavesdropping-detection-result generator is further configured to:
15 calculate a bit error rate based on the measurement of the quantum optical signal, the bit values of the control sequence, the QIDs of the first plurality of quantum state bases, the length values corresponding to the QIDs, and the second plurality of quantum state bases; and
 in response to determining that the bit error rate is less than a predetermined
20 threshold, generate an eavesdropping-detection result indicating that no eavesdropping is detected.

21. A method for detecting eavesdropping while establishing secure communication between a local node and a remote node, the method comprising:
25 generating, by the local node, a regular optical signal based on data to be transmitted;
 generating a quantum optical signal based on a control sequence and a plurality of quantum state bases, wherein the control sequence comprises a random binary bit string, and each quantum basis includes orthogonal quantum states, wherein the
30 generating comprises:
 encoding each bit of the control sequence using a randomly selected quantum state basis of the plurality of quantum state bases;

- multiplexing the regular optical signal and the quantum optical signal to produce a hybrid optical signal;
- transmitting the hybrid optical signal to the remote node;
- sending information associated with the control sequence and information
- 5 associated with the plurality of quantum state bases to the remote node; and
- receiving an eavesdropping-detection result from the remote node based on measurement of the quantum optical signal, the information associated with the control sequence, and the information associated with the plurality of quantum state bases.