ICS 01.040.35
CCS A 22

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 43692-2024

Quantum communication terminology and definition

量子通信术语和定义

Issued on: March 15, 2024 **Implemented on: October 1, 2024**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

1 Scope

The document defines the basic terms and definitions of quantum communication, comprising the general basic terms and definitions and the terms and definitions of photon-based quantum key distribution.

It applies to the drafting of quantum communication technical documents.

2 Normative references

This document has no normative references.

3 General basic terms and definitions

3.1 quantum information: the knowledge contained in the state of a quantum physical system. Source: GB/T 42565-2023, 3.2.

3.2 classical information: the knowledge contained in the state of a classical physical system. Note: it is equivalent to information in the general sense, see 4.1.1.3.8 and 4.1.1.3.9 of GB/T 4894-2009.

3.3 qubit: the smallest unit of quantum information, realised physically by a two-dimensional quantum state and expressible mathematically by a unit vector of a two-dimensional Hilbert space. Source: GB/T 42565-2023, 3.3.

3.4 logical qubit: the smallest logical unit of quantum information, which can be in a superposition of logical 0 and logical 1 and is expressible mathematically by a unit vector of a two-dimensional Hilbert space. Source: GB/T 42565-2023, 3.5.

3.5 qudit: a high-dimensional unit of quantum information, expressible mathematically by a unit vector of a D-dimensional Hilbert space.

3.6 quantum communication: the technique of conveying quantum information or classical

information by transmitting quantum states, the quantum state being the information carrier. Note: quantum communication covers several protocol schemes and application scenarios, such as quantum key distribution, quantum teleportation, quantum dense coding, quantum secure direct communication, quantum secret sharing and quantum digital signature.

3.7 quantum communication link: the physical line that connects two nodes and realises the quantum communication function.

3.8 quantum communication network: the network formed by connecting more than two nodes through quantum communication links.

3.9 quantum key distribution; QKD: the method by which the two communicating parties achieve the generation of a symmetric key through the transmission of quantum states, provided with information-theoretic security at the level of the theoretical protocol. Note: there are several quantum key distribution protocols, such as the BB84 protocol, the MDI protocol and the DI protocol among the discrete variable quantum key distribution protocols, and the GG02 protocol among the continuous variable quantum key distribution protocols. An admitted synonym is quantum key allocation.

3.10 quantum secure communication: the communication method based on quantum communication that protects secret messages by making use of properties such as the indivisibility of the quantum, the no-cloning of quantum states and quantum entanglement, and so guarantees the security of information transmission. Note 1: secret messages include keys, passwords and any sensitive information or data whose confidentiality has to be protected. Note 2: encrypted communication that combines quantum key distribution with symmetric cryptography is a typical implementation of quantum secure communication.

3.11 quantum key: the symmetric key generated directly by the two communicating parties on the basis of a quantum key distribution protocol, which can be proved to have information-theoretic security at the level of the theoretical protocol.

3.12 quantum teleportation; QT: a method for transmitting a quantum state in which a Bell state measurement is carried out on an arbitrary unknown quantum state to be transmitted together with a pre-shared entangled quantum state, and a unitary transformation is then applied to the measured entangled quantum state according to the measurement result. An admitted synonym is quantum remote transmission.

3.13 quantum dense coding: a communication method that makes use of pre-shared quantum entanglement to transmit more than one bit of classical information by sending a single qubit.

3.14 quantum secure direct communication; QSDC: a method of transmitting information directly, encoded in quantum states over a quantum channel, that achieves secure transmission by making combined use of basic principles of quantum mechanics such as the superposition of quantum states, the Heisenberg uncertainty relation, the no-cloning

theorem, the correlation of entangled particles and quantum non-locality.

3.15 quantum secret sharing; QSS: the process by which several communicating parties achieve information-theoretically secure secret sharing through the transmission of quantum states.

3.16 quantum digital signature; QDS: the process by which several communicating parties achieve an information-theoretically secure digital signature through the transmission of quantum states.

3.17 quantum signal: in quantum communication, the physical signal that carries the quantum state. Note 1: quantum communication is the physical carrier of quantum information. Note 2: quantum signals commonly used are single photons encoded or modulated on physical quantities such as polarization, phase and orbital angular momentum, and weak coherent state light encoded or modulated in phase and amplitude.

3.18 classical signal: in modern communication technology, the physical signal that carries a classical physical quantity. Note 1: it is the physical carrier of classical information. Note 2: classical signals commonly used are the high level, the low level, the bright light pulse, the dark light pulse, light pulses of different polarization states and light pulses of different phase difference.

3.19 quantum channel: the channel that transmits quantum signals.

3.20 classical channel: the channel that transmits classical signals.

3.21 preparation of quantum state(s): the process of manipulating a physical system so that its quantum state evolves or jumps to a specified quantum state.

3.22 polarization encoding: modulation over a finite number of states of the polarization degree of freedom of a photon or of weak coherent light.

3.23 phase encoding: modulation over a finite number of states of the relative phase of optical quantum states in different time modes, that is at different instants.

3.24 time-bin phase encoding: modulation over a finite number of states of the time modes of a photon or of weak coherent light and of the relative phase between different time modes.

3.25 frequency encoding: modulation over a finite number of states of the frequency degree of freedom of a photon or of weak coherent light.

3.26 gaussian modulation: in the continuous variable quantum key distribution protocol, the modulation scheme in which the sending party prepares quantum states and modulates random numbers following a gaussian distribution on the canonical components, canonical position and canonical momentum, of the quantum state.

3.27 discrete modulation: in the continuous variable quantum key distribution protocol, the

encoding scheme in which the sending party modulates random numbers on a finite number of quantum states.

3.28 modulation variance: the variance of the random numbers modulated on the canonical components of the quantum state.

3.29 single-photon source: a light source that emits only one photon at a time.

3.30 probabilistic single-photon source: a light source that emits a single photon probabilistically each time.

3.31 entangled-photon-pair source: a light source that emits photon pairs in a quantum entangled state.

3.32 heralded single-photon source: a single-photon source that generates correlated photon pairs and then uses the detection result of one of the photons to herald the generation of the other.

3.33 decoy state: a quantum signal of different intensity that a legitimate user deliberately inserts at random into the sequence of quantum signals. Note: the decoy state is used to test whether the quantum channel is under attack.

3.34 multi-photon signal: a pulse signal containing more than one photon.

3.35 mean photon number: the mean value of the number of photons contained in each optical pulse signal.

3.36 mean source power: the mean emitted optical power of the light source within a specified time interval.

3.37 weak coherent-state source: a coherent light source whose mean photon number is at the single-photon level, generally produced by attenuating coherent laser light.

3.38 source intensity: the mean photon number of the optical pulse signal emitted by the light source.

3.39 photon number distribution: the probability distribution of the number of photons contained in each optical pulse signal.

3.40 phase randomization: in QKD based on a weak coherent state pulsed light source, the behaviour by which the sending party makes the phase of the weak coherent state light pulses vary at random.

3.41 detection of quantum state(s): the process of carrying out a quantum state measurement on a physical system and obtaining a macroscopic physical signal that expresses the measurement result.

3.42 quantum state measurement: the process of measuring a quantum state so as to obtain the value of an observable physical quantity. Note: quantum state measurement is