Chinastandards.org

ICS 35.030
CCS L 80

GM

GM/T 0108-2021

Decoy-state BB84 quantum key distribution product technology specification

诱骗态BB84量子密钥分配产品技术规范

(English Translation)

Issued on: October 18, 2021 **Implemented on: May 1, 2022**

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0108-2021

Chinastandards.org

Table of Contents

Position of quantum key distribution products in quantum secure communication system .. 1
Description of basis and state 2
Selection of basis and state 3
Decoding 4
Detection 5
Parameter estimation 6
Parameter estimation 7
Error correction 8
Privacy amplification 9
Safety design requirements 10
Identification requirements 11
Interface requirements 12
Random number generator 13
Log management 14
Remote management 15

5.1 Position of quantum key distribution products in quantum secure communication system

5.2 Network deployment of quantum key distribution products... 11

6 Requirements for implementing the decoy-state BB84 protocol... 13

6.1 Overview and protocol flow... 13

6.2 Protocol implementation... 14

7 Product requirements for quantum key distribution... 24

7.1 Basic requirements... 24

7.2 Identification requirements... 25

7.3 Interface requirements... 25

7.4 Random number generator... 26

7.5 Log management... 26

7.6 Remote management... 26 Annex A (informative) Introduction to the decoy-state BB84

Preview: page 2 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0108-2021

protocol... 27 Annex B (informative) Composition structure of quantum key distribution products 28 Annex C (informative) Requirements for defense against attacks and protective measures... 30 Annex D (informative) Error correction methods... 32 Annex E (informative) Methods for privacy amplification... 34 Annex F (informative) Calculation formula of compression ratio during privacy amplification process... 37 Bibliography... 40 Decoy-state BB84 quantum key distribution product technology specification

1 Scope

Based on the BB84 protocol using weak coherent state light sources, this document specifies the technical implementation of each stage of the protocol and puts forward basic requirements for the design of products using this protocol.

This document is applicable to the development and testing of quantum key distribution products based on the decoy-state BB84 protocol.

2 Normative references the following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GB/T 2423.1, Environmental testing for electric and electronic products -- Part 2:

Test methods -- Tests A: Cold GB/T 2423.2, Environmental testing for electric and electronic products -- Part 2:

Test methods -- Tests B: Dry heat GB/T 15843.2, Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms GB/T 15843.4, Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function GB/T 15852.1, Information technology. Security techniques -- Message authentication codes -- Part 1: Mechanisms using a block cipher GB/T 15852.2, Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function GB/T 15852.3, Information technology -- Security techniques -- Message authentication codes (MACs) -- Part 3: Mechanisms using a universal hash-function GB/T 32915, Information security technology -- Randomness test methods for binary sequence A complete description of the motion state of a physical system in quantum mechanics.

It can be represented by a vector in Hilbert space.

3.18 quantum channel A channel for transmitting quantum states.

3.19 quantum information the information contained in the quantum system. Its characteristics must be described and explained using quantum mechanics.

3.20 sifted key

Preview: page 3 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0108-2021

The data obtained after the original key is based (screened).

3.21 signal state

Quantum states used to load classical bit information.

3.22 phase randomization the process in which the sending end randomly modulates the phase of weak coherent light.

3.23 phase error rate the rate at which a quantum bit undergoes phase-flip errors. This value is used to estimate the amount of key information that an eavesdropper might know.

3.24 decoy state

A quantum state that differs from the signal state only in intensity and modulation information, but has the same other physical quantities such as frequency domain and time domain characteristics.

3.25 decoy-state BB84 protocol Based on the BB84 protocol, it uses a variety of random light intensities to monitor the channel and estimate the single-photon state characteristics, thereby solving the security problem based on non-ideal single-photon sources. For an introduction to the decoy-state BB84 protocol, see Annex A.

3.26 raw key

The original data obtained after the quantum signal is measured by the receiving end.

3.27 maximal distance

a) Quantum state preparation: the sending end prepares quantum states as information carriers. The quantum states used to load information are randomly loaded onto the corresponding light pulses. Quantum states can be characterized by physical quantities such as polarization, phase, time, spin, and momentum.

b) Quantum state transmission: the sending end sends the quantum state loaded with information to the receiving end.

c) Quantum state measurement: the receiving end randomly selects a measurement basis to measure the quantum state loaded with information sent by the sending end to generate a raw key.

d) Basis sifting: the sending end and receiving end compare the coding basis used in the preparation of the quantum state with the measurement basis used by the receiving end for detection. Both parties only retain the data using the same basis vector to generate a sifted key.

e) Error correction: the sending end and receiving end correct the quantum bit errors in the sifted key at both ends to generate an error-corrected key.

f) Privacy amplification: the sending end and receiving end compress the error-corrected

Preview: page 4 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0108-2021

key by calculating the compression ratio to generate a shared key.

6.2.1.1 Description of basis and state

Description of states: the four quantum states defining the two-dimensional Hilbert space are denoted as |phi1 >, |phi2 >, |psi1 >, and |psi2 >.

Description of basis: define two sets of basis of the two-dimensional Hilbert space, denoted by Phi and Psi, with Phi = {|phi1 >, |phi2 >}, Psi = {|psi1 >, |psi2 >}.

Information convention: when selecting a basis, define the basis Phi to correspond to the classical bit "0"; the basis Psi to correspond to the classical bit "1".

When the basis is Phi, the quantum state |phi1 > is defined to correspond to the classical bit "0", and the quantum state |phi2 > corresponds to the classical bit "1".

When the basis is chosen as Psi, the quantum state |psi1 > is defined to correspond to the classical bit "0", and the quantum state |psi2 > corresponds to the classical bit "1".

6.2.1.2 Selection of basis and state

through the quantum channel in accordance with the requirements of 6.2.1 of this standard. It records the light intensity of the emitted pulse to prepare information and code information.

6.2.3.1 Decoding

The decoding process is that the receiving end randomly selects a measurement basis to demodulate the quantum state loaded with information sent by the sending end.

The decoding process shall meet the following requirements:

According to the physical random sequence output by the random number generator, through the correspondence between binary bits 0, 1 and the basis agreed in 6.2.1.1, select the measurement basis used to measure the quantum state and demodulate the quantum state. The preparation of the measurement basis shall comply with the requirements of 6.2.1.3. The ratio of the number of preparations of the two groups of basis shall be in accordance with the preset requirements of the product.

During the decoding process, if the receiving end uses an active basis selection scheme, it shall at least have the ability to resist Trojan horse attacks.

During the decoding process, if the receiving end is actively selecting a basis (not selecting a state), it shall at least be able to resist fluorescence attacks. If the receiving end is actively selecting a basis (not selecting a state) and using multiple detectors, it shall at least be able to resist forged state attacks, time displacement attacks, and device calibration attacks.

During the decoding process, if the receiving end adopts a passive basis selection scheme,

Preview: page 5 of 5 shown, 40 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0108-2021