Chinastandards.org

ICS 35.030

GM

GM/T 0114-2021

Decoy-state BB84 quantum key distribution product test specification

诱骗态BB84量子密钥分配产品检测规范

(English Translation)

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

Issued by: State Administration of Cryptography

Preview: page 1 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0114-2021

Chinastandards.org

Table of Contents

Scope 1
Normative references 2
Terms and definitions 3
Symbols 4
Test reference point 5
Basis (state) preparation detection environment topology diagram 6
Topology diagram of the other attribute preparation detection environment 7
Topology diagram of key attribute detection environment of detector 8
Topology diagram of remote management detection environment 9
Overview 10
Basis preparation 11
State preparation 12
Coding process 13
Detection of quantum state transmission process 14
Decoding process 15
Authentication testing 16
Interface detection 17
Detection of random number generator 18
Relative error of conjugation of measurement basis 19
Amplitudes of various quantum states in signal state 20
Laser injection attack protection 21
Protection against seed light injection attacks 22
Qualification judgment 23

1 Scope

This document specifies the detection content and methods of the protocol implementation requirements and basic product requirements of the decoy-state BB84 quantum key distribution product, based on the use of weak coherent state light source.

This document is applicable to the detection of decoy-state BB84 quantum key distribution products, which are developed in accordance with GM/T 0108-2021; it can also be used to guide the development. The system security based on quantum key distribution products and the security of their classical channel networks are not within the scope of this

Preview: page 2 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0114-2021

document.

2 Normative references

The contents of the following documents constitute the essential provisions of this document through normative references in the text. Among them, for referenced documents with dates, only the version corresponding to that date applies to this document; for referenced documents without dates, the latest version (including all amendments) applies to this document.

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 5080.7 Equipment reliability testing - Compliance test plans for failure rate and mean time between failures assuming constant failure rate

3 Terms and definitions

The terms and definitions defined in GB/T 37092, GM/T 0050, GM/Z 4001 apply to this document.

Privacy amplification the process in which the transmitter and the receiver perform mathematical processing on the error-corrected key to extract the shared key from it.

BB84 protocol

A quantum key distribution protocol proposed by Charles Henry Bennett and Gilles Brassard in 1984.

Basis sifting

Also called sifting, it refers to the process in which the transmitter and receiver compare the basis vectors; both parties only retain the data that uses the same basis vectors in the measurement process of the receiver and the sending process of the transmitter.

Basis

A set of quantum states consisting of N complete orthogonal normalized quantum states in the N-dimensional Hilbert space.

4.1 Symbols

The following symbols apply to this document.

μ. Average number of photons in signal state light pulse

Preview: page 3 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0114-2021

5.1 Test reference point

The reference configuration of the decoy-state BB84 quantum key distribution product is shown in Figure 1, where the QKD transmitter includes a light source, a decoy-state preparation module, a ground/state preparation module, a light intensity attenuation module, a random number generator, a transmitter control module, a synchronization signal transmission module, a negotiation signal transceiver module, a communication control interface module.

5.2.1.1 Basis (state) preparation detection environment topology diagram

Figure 2 shows the coding basis relative error detection environment of the phase-coded

quantum key distribution product, which is mainly composed of the QKD transmitter, circulator, single photon detector, reflector. If the QKD transmitter base/state preparation module adopts a single-mode Faraday-Michelson interferometer, the

5.2.1.3 Topology diagram of the other attribute preparation detection environment

Figure 8 is the detection environment for various quantum state amplitudes and pulse

widths, which is mainly composed of the QKD transmitter, the photoelectric converter, the oscilloscope. This detection environment is used for the detection of 6.1.1.5.

5.2.1.4 Topology diagram of key attribute detection environment of detector

Figure 11 is the detection environment of key attribute of detector, which is mainly

composed of narrow pulse light source, signal source, (QKD receiver) single photon detector, adjustable attenuator, pulse counter. It can perform detection efficiency half-width consistency detection, efficiency peak consistency detection, etc. This detection environment is used for the detection of 6.1.3.2.

5.2.2.4 Topology diagram of remote management detection environment

Figure 19 is the detection environment of remote management, which is mainly

composed of QKD transmitter, QKD receiver, detection PC. This detection environment is used for the detection of 6.2.6.

6.1.1.1 Overview

State description. Define the four quantum states of the two-dimensional Hilbert space as |phi1 >, |phi2 >, |Psi1 >, |Psi2 >.

Preview: page 4 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0114-2021

6.1.1.2 Basis preparation

The purpose of the basis preparation test is to detect whether the two sets of bases prepared by the transmitter and the receiver meet the requirements of the decoy-state BB84 protocol. The basis preparation error detection includes the relative error detection of the conjugation of the encoding basis, the relative error detection of the conjugation of the measurement basis, the relative error detection of the encoding basis and the measurement basis.

6.1.1.3 State preparation

The purpose of state preparation detection is to detect whether the two quantum states of each group of bases prepared by the transmitter and the receiver meet the requirements of the decoy-state BB84 protocol.

6.1.1.6 Coding process

The purpose of the coding process detection is to detect whether the transmitter coding process meets the requirements of the decoy-state BB84 protocol.

6.1.2 Detection of quantum state transmission process

The purpose of the detection of quantum state transmission process is to detect whether the quantum state transmission process meets the requirements of the decoy-state BB84 protocol.

6.1.3.1 Decoding process

The purpose of the decoding process detection is to detect whether the decoding process of the receiver meets the requirements of the decoy-state BB84 protocol.

6.2.2 Authentication testing

The purpose of authentication testing is to detect the authentication mechanism used between the transmitter and the receiver of the quantum key distribution product, and between the quantum key distribution product and the shared key management system, management platform or management tool.

6.2.3 Interface detection

The purpose of interface detection is to detect whether the type and function of the interface of the quantum key distribution product meet the requirements of the quantum key distribution product.

Preview: page 5 of 5 shown, full document available. Complete English PDF, instant download:
https://chinastandards.org/standards/gm-t-0114-2021