ICS 35.030
L 80

GM

中华人民共和国密码行业标准

GM/T 0114—2021

诱骗态 BB84 量子密钥分配产品检测规范

Decoy-state BB84 quantum key distribution product test specification

2021-10-18 发布　　2022-05-01 实施

国家密码管理局　　发 布

目　　次

前　言

本文件依据 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：安徽问天量子科技股份有限公司、国家密码管理局商用密码检测中心、中国科学技术大学、中国人民解放军信息工程大学、江苏亨通问天量子信息研究院有限公司、中国电子科技集团第三十研究所、科大国盾量子技术股份有限公司、重庆大学、北京邮电大学、兴唐通信科技有限公司。

本文件主要起草人：刘婧婧、韩正甫、刘云、宋晨、邓开勇、雷银花、徐锦丽、吕春梅、苗春华、刘杰杰、张启发、凌杰、宋欢欢、银振强、陈巍、李宏伟、赵良圆、徐兵杰、何远杭、赵梅生、唐世彪、向宏、蔡斌、喻松、张一辰、于宗文、李申。

诱骗态 BB84 量子密钥分配产品检测规范

1 范围

本文件规定了基于采用弱相干态光源的诱骗态 BB84 量子密钥分配产品的协议实现要求和产品基本要求的检测内容和方法。

本文件适用于指导符合 GM/T 0108—2021 研制的诱骗态 BB84 量子密钥分配产品的检测，也可用于指导研制。基于量子密钥分配产品的系统安全及其经典信道网络安全不属于本文件规定的范围。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 2423.1 电工电子产品环境试验 第 2 部分：试验方法 试验 A：低温

GB/T 2423.2 电工电子产品环境试验 第 2 部分：试验方法 试验 B：高温

GB/T 5080.7 设备可靠性试验 恒定失效率假设下的失效率与平均无故障时间的验证试验方案

GB/T 15843.2 信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制

GB/T 15843.4 信息技术 安全技术 实体鉴别 第 4 部分：采用密码校验函数的机制

GB/T 15852.1 信息技术 安全技术 消息鉴别码 第 1 部分：采用分组密码的机制

GB/T 15852.2 信息技术 安全技术 消息鉴别码 第 2 部分：采用专用杂凑函数的机制

GB/T 15852.3 信息技术 安全技术 消息鉴别码 第 3 部分：采用泛杂凑函数的机制

GB/T 32915 信息安全技术 二元序列随机性检测方法

GB/T 37092 信息安全技术 密码模块安全要求

GB/T 38625 信息安全技术 密码模块安全检测要求

GM/T 0062 密码产品随机数检测要求

GM/T 0108—2021 诱骗态 BB84 量子密钥分配产品技术规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 37092、GM/T 0050 和 GM/Z 4001 界定的术语和定义适用于本文件。

3.1

安全增强 privacy amplification

发送端与接收端对纠错后密钥进行数学处理，从中提取共享密钥的过程。

3.2

BB84 协议 BB84 protocol

由 Charles Henry Bennett 和 Gilles Brassard 在 1984 年提出的量子密钥分配协议。

3.3

对基 basis sifting

也称作筛选，是指发送端与接收端进行基矢比对，双方只保留接收端测量过程与发送端发送过程时

所使用了相同基矢的数据的过程。

3.4

基　basis

N 维希尔伯特空间中，N 个完备正交归一量子态组成的量子态集合。

3.5

纠错　error correction

对发送端与接收端筛后密钥中量子比特误码进行纠正的过程。

3.6

纠错后密钥　corrected key

筛后密钥经过纠错之后获得的数据。

3.7

经典信道　classical channel

传输除量子态以外的其他信息的信道。

3.8

量子比特误码　quantum error bit

发送端与接收端的筛后密钥中不一致的数据比特，也称作误码。

3.9

共享密钥　shared key

采用量子密钥分配协议所产生的对称密钥。

3.10

量子密钥分配　quantum key distribution

也称作量子密钥协商或量子密钥分发，是密码学与量子力学结合的产物，利用量子力学原理，以量子态为载体通过量子信道实现异地间协商对称密钥。

3.11

量子密钥分配产品　quantum key distribution product

具有量子密钥分配功能的产品。

3.12

共享密钥生成率　shared key rate

量子密钥分配产品在单位时间内生成的共享密钥量的比率。

3.13

量子态　quantum state

量子力学中对物理系统运动状态的完备描述，可用希尔伯特空间的一个向量表示。

3.14

量子信道　quantum channel

传输量子态的信道。

3.15

量子信息　quantum information

量子体系所蕴含的信息，其特性必须使用量子力学进行描述和解释。

3.16

筛后密钥　sifted key

原始密钥经对基(筛选)之后获得的数据。

3.17

信号态　signal state

用以加载经典比特信息的量子态。

3.18

希尔伯特空间　hilbert space

一个完备的内积空间，是数学和量子力学的关键性概念之一。

3.19

相位随机化　phase randomization

发送端对弱相干光的相位进行随机调制的过程。

3.20

诱骗态　decoy state

与信号态相比，仅强度和调制信息不同，但频域、时域特性等其他物理量都相同的量子态。

3.21

诱骗态 BB84 协议　decoy-state BB84 protocol

基于 BB84 协议，采用多种随机的光强来监测信道并估计单光子态特性，从而解决基于非理想单光子源的安全性问题的协议。

3.22

原始密钥　raw key

量子信号经接收端测量之后获得的原始数据。

3.23

最大距离　maximal distance

在满足量子密钥分配产品性能和安全需求的前提下，发送端与接收端之间量子信道的最大长度。

4　符号和缩略语

4.1　符号

下列符号适用于本文件。

μ　信号态光脉冲的平均光子数

ν_1　诱骗态 1 光脉冲的平均光子数

ν_2　诱骗态 2 光脉冲的平均光子数

4.2　缩略语

下列缩略语适用于本文件。

APD　雪崩光电二极管(Avalanche Photon Diode)

QKD　量子密钥分配(Quantum Key Distribution)

5　检测环境

5.1　测试参考点

诱骗态 BB84 量子密钥分配产品的参考配置如图 1 所示，其中 QKD 发送端包含光源、诱骗态制备模块、基/态制备模块、光强衰减模块、随机数发生器、发送端控制模块、同步信号发送模块、协商信号收发模块和通信控制接口模块等。QKD 接收端包含线路适配补偿模块、量子态解调模块、探测模块、随机数发生器、接收端控制模块、同步信号接收模块、协商信号收发模块和通信控制接口模块等。

针对诱骗态 BB84 量子密钥分配产品检测过程中所使用的陪测设备，可参见附录 A。

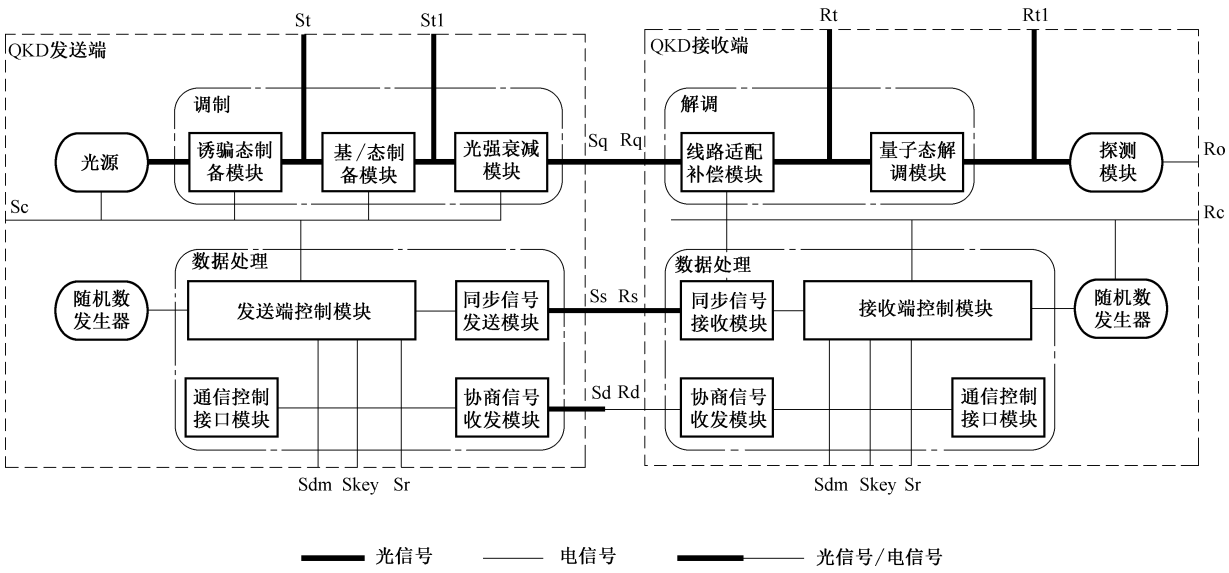

图 1　量子密钥分配产品配置和测试参考点

定义了 16 个测试参考点，即 St，St1，Sc，Sq，Ss，Sd，Rt，Rt1，Rc，Ro，Rq，Rs，Rd，Sr，Sdm，Skey。其中，St 是 QKD 发送端基/态制备之前的光脉冲信号的参考点。St1 是经过基/态制备的光脉冲信号的参考点。Sc 和 Rc 是 QKD 发送端和接收端的同步时钟电信号的参考点，可用于提供 QKD 产品测试的同步时钟信号。Sq 是 QKD 发送端经量子态制备之后的量子光信号的参考点，Rq 是 QKD 接收端的接收量子光信号的参考点，Sq 和 Rq 可用于量子光参数测试。Rt、Rt1 是 QKD 接收端量子态解码前后的参考点。Ss 和 Rs 是 QKD 发送端和接收端的同步光信号的参考点，可作为 Sc 的备用参考点。Ro 是 QKD 接收端探测模块的探测输出电信号的参考点，可用于接收端探测模块测试。Sd 和 Rd 是 QKD 发送端和接收端的协商信号的参考点。Sr 是随机数输出的参考点。Sdm 是设备管理的参考点。Skey 是量子密钥输出的参考点。

5.2　检测环境

5.2.1　协议实现要求检测

5.2.1.1　基(态)制备检测环境拓扑图

图 2 为相位编码量子密钥分配产品的编码基相对误差检测环境，主要由 QKD 发送端、环形器、单光子探测器和反射镜组成。如果 QKD 发送端基/态制备模块采用单模的法拉第-迈克尔逊干涉仪，则反射镜应采用法拉第反射镜；如果 QKD 发送端基/态制备模块采用保偏光纤的马赫-曾德尔干涉仪，则反射镜应采用保偏反射镜。该检测环境用于 6.1.1.2 和 6.1.1.3 的检测。

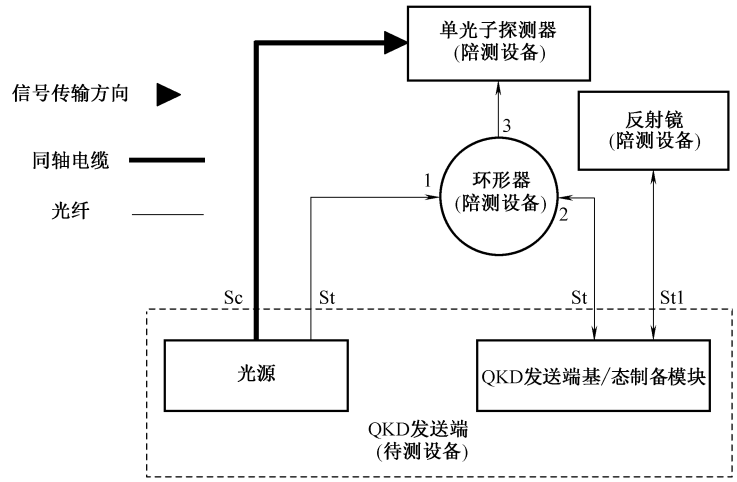

图 2　编码基相对误差检测环境拓扑图(相位编码)

图 3 为偏振编码量子密钥分配产品的编码基相对误差检测环境,主要由 QKD 发送端和偏振分析仪组成。该检测环境用于 6.1.1.2 和 6.1.1.3 的检测。

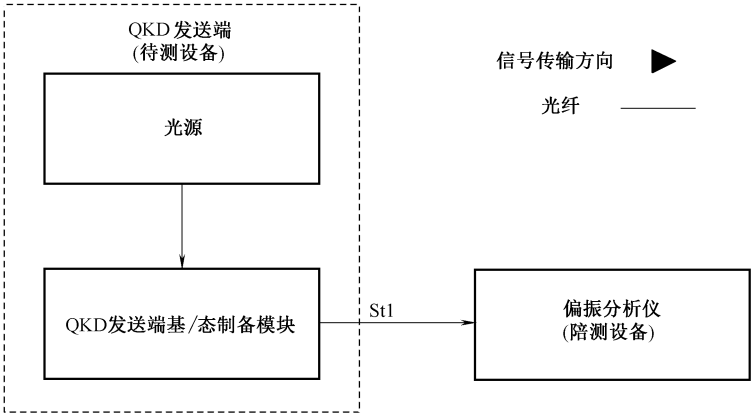

图 3　编码基相对误差检测环境拓扑图(偏振编码)

图 4 为相位编码量子密钥分配产品的测量基相对误差检测环境,主要由 QKD 发送端、QKD 接收端、环形器、单光子探测器和反射镜组成。如果 QKD 发送端基/态制备模块采用单模的法拉第-迈克尔逊干涉仪,则反射镜应采用法拉第反射镜;如果 QKD 发送端基/态制备模块采用保偏光纤的马赫-曾德尔干涉仪,则反射镜应采用保偏反射镜。该检测环境用于 6.1.1.2 和 6.1.1.3 的检测。

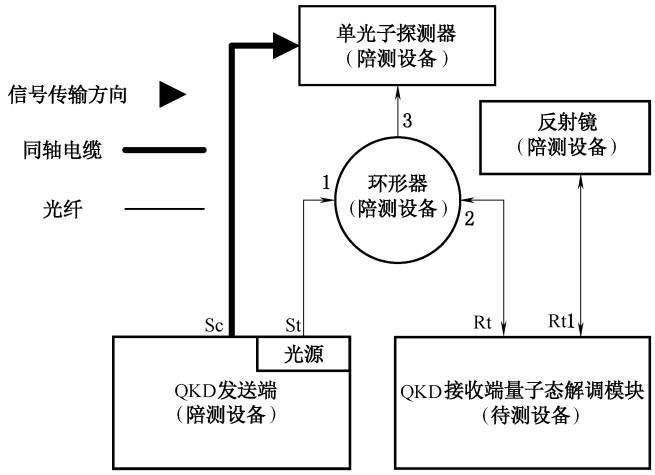

图 4　测量基相对误差检测环境拓扑图(相位编码)

图 5 为偏振编码量子密钥分配产品的测量基相对误差检测环境，主要由 QKD 发送端、QKD 接收端、光功率计/偏振分析仪组成。该检测环境用于 6.1.1.2 和 6.1.1.3 的检测。

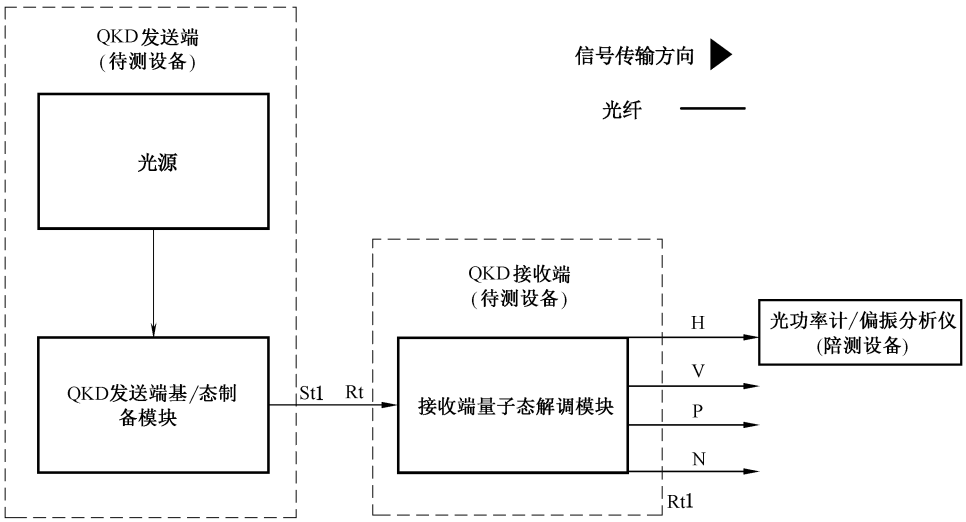

图 5　测量基相对误差检测环境拓扑图(偏振编码)

图 6 为量子密钥分配产品的编码基与测量基相对误差检测环境，主要由 QKD 发送端、QKD 接收端、网络交换机和检测用 PC 组成。该检测环境用于 6.1.1.2 的检测。

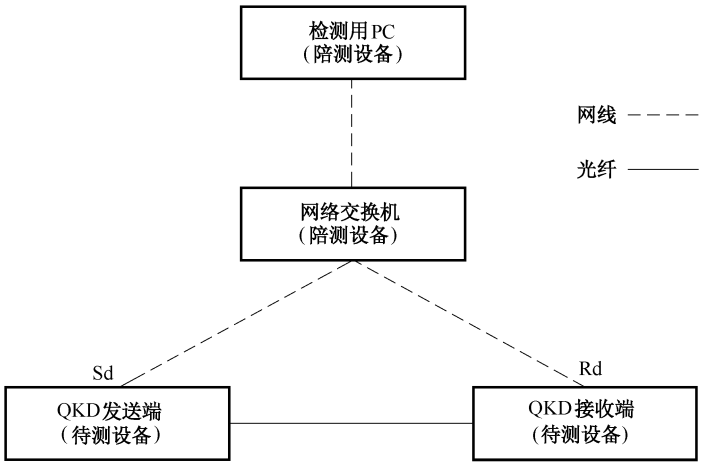

图 6　编码基与测量基相对误差检测环境拓扑图

5.2.1.2　光强制备检测环境拓扑图

图 7 为光强制备检测环境，主要由 QKD 发送端、检测用 PC 和光功率计组成。该检测环境用于 6.1.1.4 的检测。

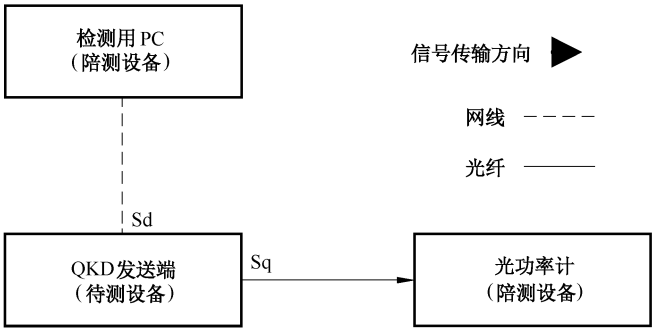

图 7　光强制备检测环境拓扑图

5.2.1.3　其他属性制备检测环境拓扑图

图 8 为各种量子态幅度和脉宽的检测环境，主要由 QKD 发送端、光电转换器和示波器组成。该检测环境用于 6.1.1.5 的检测。

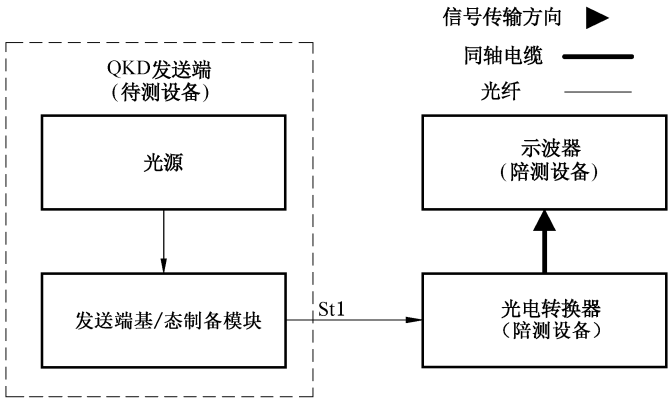

图 8　各种量子态幅度/脉宽检测环境拓扑图

图 9 为各种量子态光谱的检测环境，主要由 QKD 发送端和光谱分析仪组成。该检测环境用于 6.1.1.5 的检测。

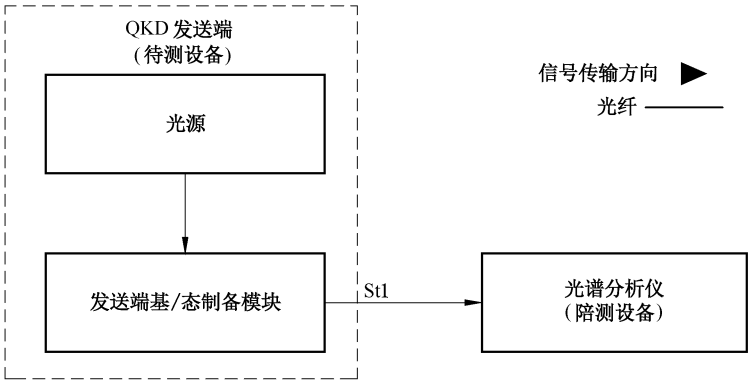

图 9　各种量子态光谱检测环境拓扑图

图 10 为各种量子态时间的检测环境，主要由 QKD 发送端、光电转换器和示波器组成。该检测环境用于 6.1.1.5 的检测。

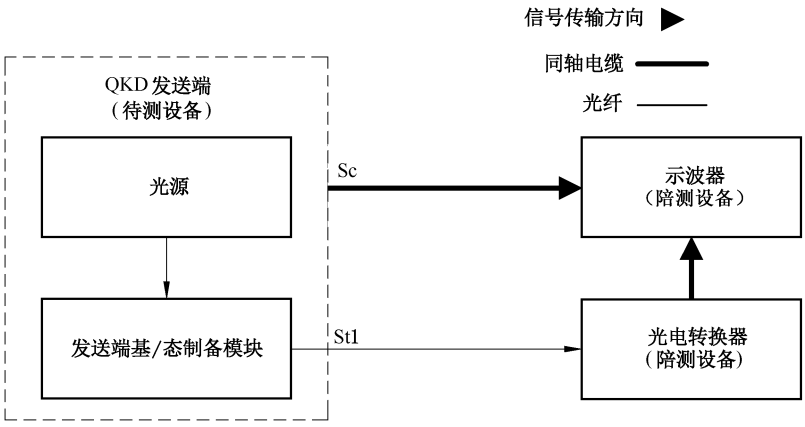

图 10　各种量子态时间检测环境拓扑图

5.2.1.4 探测器关键属性检测环境拓扑图

图 11 为探测器关键属性的检测环境，主要由窄脉冲光源、信号源、(QKD 接收端)单光子探测器、可调衰减器和脉冲计数器组成。可进行探测效率半高宽一致性检测、探测效率峰值一致性检测等。该检测环境用于 6.1.3.2 的检测。

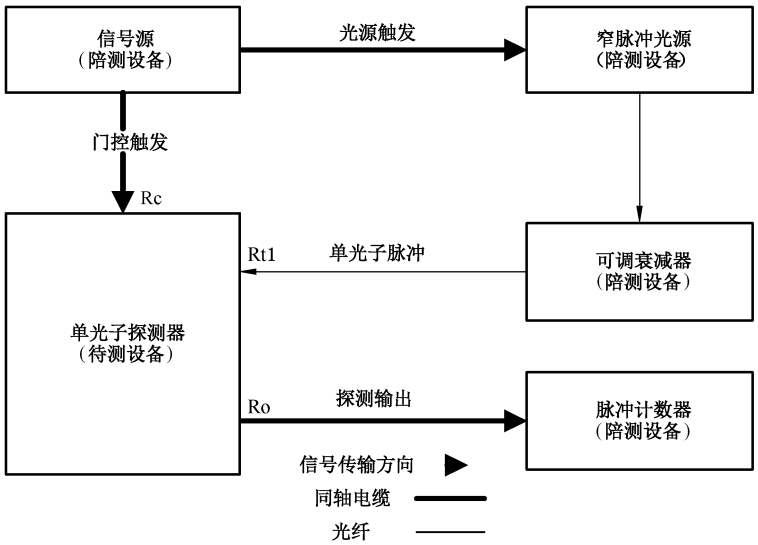

图 11 探测器关键属性检测环境拓扑图

5.2.1.5 防攻击检测环境拓扑图

图 12 为强光攻击防护的检测环境，主要由 QKD 发送端、QKD 接收端、光源合束器、可调衰减器、连续波光源和脉冲计数器组成。该检测环境用于 6.1.3.2 的检测。

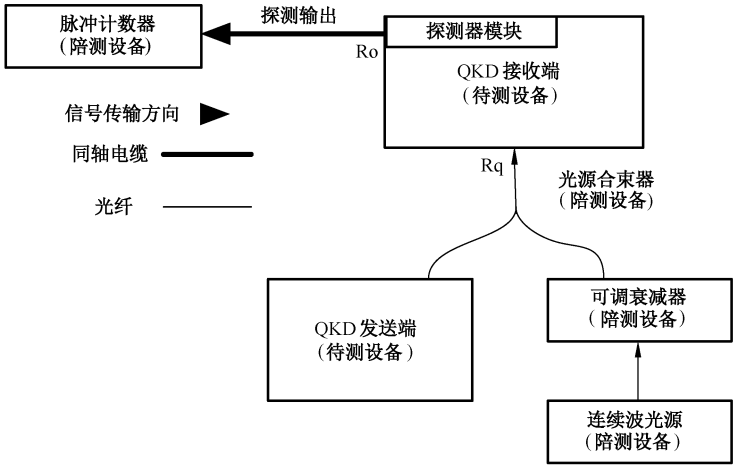

图 12 强光攻击防护检测环境拓扑图

图 13 为双计数攻击防护的检测环境，主要由 QKD 发送端、QKD 接收端、光源合束器、可调衰减器和脉冲光源组成，脉冲光源与 QKD 发送端应存在同步机制。该检测环境用于 6.1.3.2 的检测。

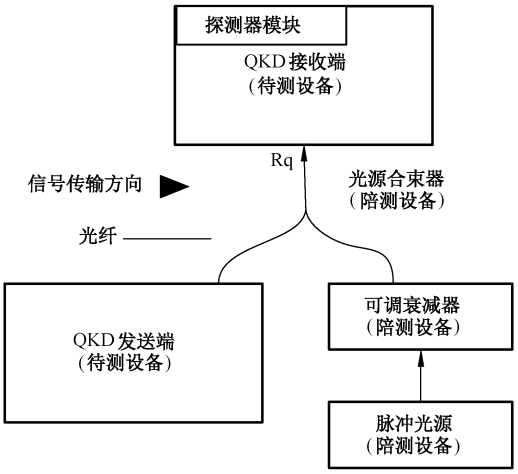

图 13　双计数攻击防护检测环境拓扑图

图 14 为设备校准攻击防护的检测环境，主要由 QKD 发送端、QKD 接收端、光源合束器、可调衰减器和光源组成。该检测环境用于 6.1.3.2 的检测。

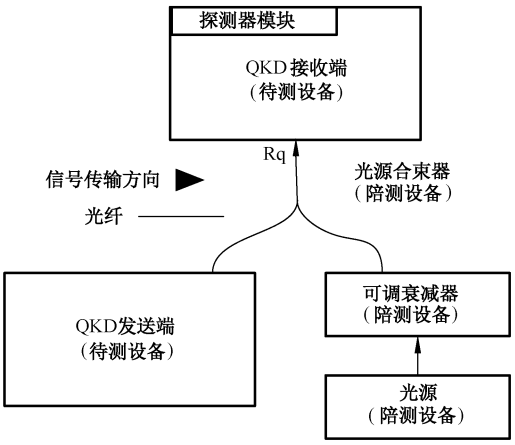

图 14　设备校准攻击防护检测环境拓扑图

5.2.1.6　对基、纠错、安全增强过程检测环境拓扑图

图 15 为对基、纠错、安全增强过程的检测环境，主要由 QKD 发送端、QKD 接收端、检测用 PC 和集线器组成。也可通过串口、USB 或者其他形式的测试接口导出测试数据。该检测环境用于 6.1.4、6.1.5 和 6.1.6 的检测。

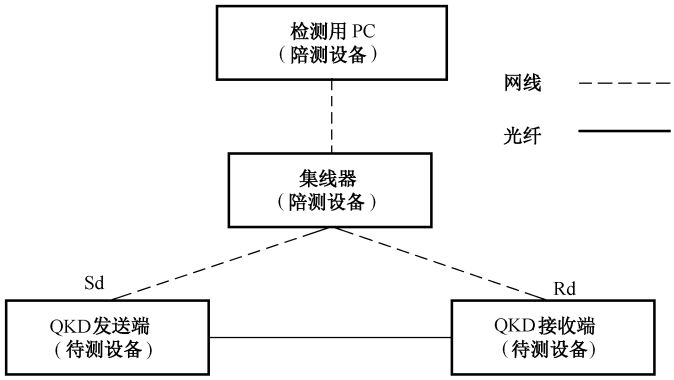

图 15　对基、纠错、安全增强过程检测环境拓扑图

5.2.2　量子密钥分配产品检测

5.2.2.1　功能检测环境拓扑图

图 16 为共享密钥随机性和一致性的检测环境，主要由 QKD 发送端、QKD 接收端和检测用 PC 组成。也可通过串口、USB 或者其他形式的测试接口导出测试数据。该检测环境用于 6.2.1.1 的检测。

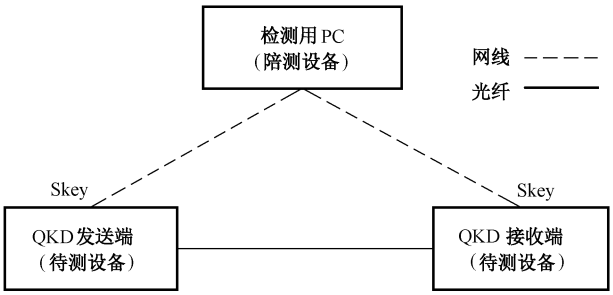

图 16　共享密钥随机性和一致性检测环境拓扑图

5.2.2.2　性能检测环境拓扑图

图 17 为共享密钥生成率和最大距离的检测环境，主要由 QKD 发送端、QKD 接收端、可调衰减器、光纤盘和检测用 PC 组成。也可通过串口、USB 或者其他形式的测试接口导出测试数据。该检测环境用于 6.2.1.2.1 和 6.2.1.2.2 的检测。

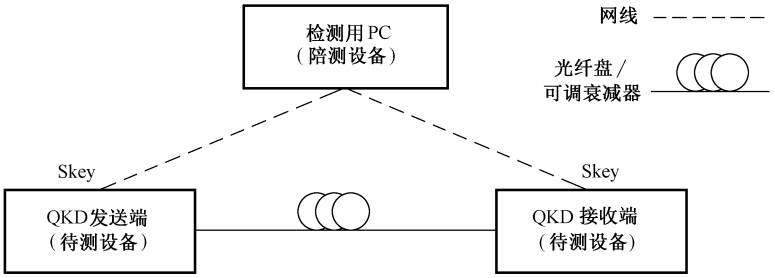

图 17　共享密钥生成率和最大距离检测环境拓扑图

5.2.2.3 随机数发生器检测环境拓扑图

图 18 为随机数发生器的检测环境，主要由 QKD 发送端、QKD 接收端和检测用 PC 组成。也可通过串口、USB 或者其他形式的测试接口导出测试数据。该检测环境用于 6.2.4 的检测。

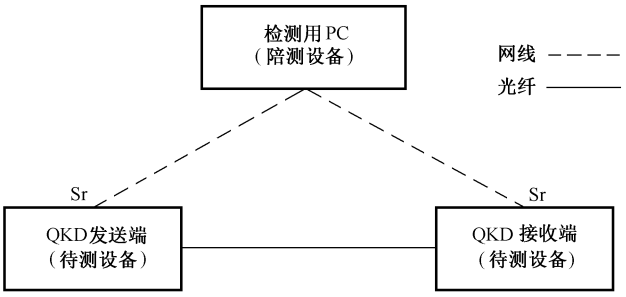

图 18 随机数发生器检测环境拓扑图

5.2.2.4 远程管理检测环境拓扑图

图 19 为远程管理的检测环境，主要由 QKD 发送端、QKD 接收端和检测用 PC 组成。该检测环境用于 6.2.6 的检测。

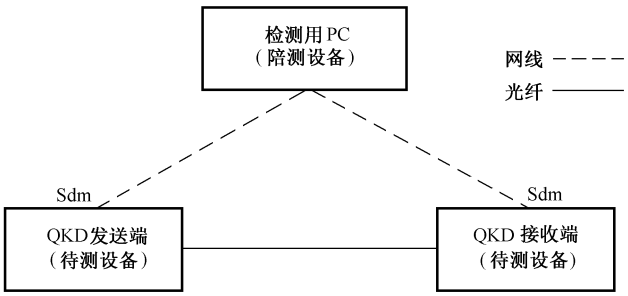

图 19 远程管理检测环境拓扑图

6 检测内容

6.1 协议实现要求检测

6.1.1 量子态制备

6.1.1.1 概述

态的描述：定义二维希尔伯特空间的四种量子态分别记为$|\varphi_1\rangle$、$|\varphi_2\rangle$、$|\Psi_1\rangle$、$|\Psi_2\rangle$。

基的描述：定义二维希尔伯特空间的两组基分别记为与 Φ 与 Ψ，且 $\Phi=\{|\varphi_1\rangle,|\varphi_2\rangle\}$，$\Psi=\{|\Psi_1\rangle,|\Psi_2\rangle\}$。

信息约定：在选基时，定义基 Φ 与经典比特“0”对应；基 Ψ 与经典比特“1”对应。当基选择 Φ 时，定义量子态$|\varphi_1\rangle$与经典比特“0”对应；量子态$|\varphi_2\rangle$与经典比特“1”对应；当基选择 Ψ 时，定义量子态$|\Psi_1\rangle$与经典比特“0”对应；量子态$|\Psi_2\rangle$与经典比特“1”对应。

发送端和接收端选择二维希尔伯特空间中两组标准正交基，且这两组基互为共轭。发送端制备的两组基称为编码基，接收端制备的两组基称为测量基。每组基包含两个正交的量子态，即发送端应制备四种量子态。

6.1.1.2 基制备

基制备检测的目的是检测发送端、接收端制备的两组基是否符合诱骗态 BB84 协议的要求。基制备误差检测包括编码基共轭性相对误差检测、测量基共轭性相对误差检测和编码基与测量基的相对误差检测。

两组基共轭，即 Φ 和 Ψ 共轭。

定义 1：记 $A=|\langle\varphi_1|\Psi_1\rangle|$，$B=|\langle\varphi_1|\Psi_2\rangle|$，$C=|\langle\varphi_2|\Psi_1\rangle|$，$D=|\langle\varphi_2|\Psi_2\rangle|$，理论值均为 $E=\frac{1}{\sqrt{2}}$，偏离共轭性相对误差定义为 $\frac{\max(|A-E|,|B-E|,|C-E|,|D-E|)}{E}$。

定义 2：发送端的两组基分别记为 Φ^A 与 Ψ^A，其中 $\Phi^A=\{|\varphi_1^A\rangle,|\varphi_2^A\rangle\}$，$\Psi=\{|\Psi_1^A\rangle,|\Psi_2^A\rangle\}$，接收端与之对应的两组基分别记为 Φ^B 与 Ψ^B，其中 $\Phi^B=\{|\varphi_1^B\rangle,|\varphi_2^B\rangle\}$，$\Psi^B=\{|\Psi_1^B\rangle,|\Psi_2^B\rangle\}$。记 $\varepsilon_1=\cos^{-1}|\langle\varphi_1^A|\varphi_1^B\rangle|$，$\varepsilon_2=\cos^{-1}|\langle\varphi_2^A|\varphi_2^B\rangle|$，$\varepsilon_3=\cos^{-1}|\langle\Psi_1^A|\Psi_1^B\rangle|$，$\varepsilon_4=\cos^{-1}|\langle\Psi_2^A|\Psi_2^B\rangle|$。编码基与测量基的相对误差定义为 $\frac{2}{\pi}\max(\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4)$。

要求：

a) 编码基共轭性相对误差应小于 10%；

b) 测量基共轭性相对误差应小于 10%；

c) 编码基与测量基的相对误差应小于 10%。

6.1.1.3 态制备

态制备检测的目的是检测发送端、接收端制备的每组基的两种量子态是否符合诱骗态 BB84 协议的要求。

定义：$|\varphi_1\rangle$ 与 $|\varphi_2\rangle$ 的正交误差定义为 $\varepsilon=\frac{\pi}{2}-\theta$，其中 $\theta=\arccos|\langle\varphi_1|\varphi_2\rangle|$；$|\Psi_1\rangle$ 与 $|\Psi_2\rangle$ 的正交误差定义为 $\varepsilon'=\frac{\pi}{2}-\theta'$，其中 $\theta'=\arccos|\langle\Psi_1|\Psi_2\rangle|$。

要求：

a) $|\varphi_1\rangle$ 与 $|\varphi_2\rangle$ 的正交误差应符合：

$$\varepsilon/\frac{\pi}{2}<10\%$$

b) $|\Psi_1\rangle$ 与 $|\Psi_2\rangle$ 的正交误差应符合：

$$\varepsilon'/\frac{\pi}{2}<10\%$$

6.1.1.4 光强制备

光强制备检测的目的是检测发送端制备的光脉冲强度是否符合诱骗态 BB84 协议的要求。

发送端制备量子态作为量子信息的载体。以诱骗态协议中常使用的三态协议为例，量子态光脉冲具有三种不同强度，可分别作为信号态、诱骗态 1、诱骗态 2。

要求：

a) 信号态、诱骗态 1、诱骗态 2 光脉冲的强度应符合 $0\leqslant\nu_2<\nu_1<\mu$；

b) 同种强度的量子态应符合：

$$\left|\frac{p'-p}{p}\right|<20\%$$

式中：

p'——实际光脉冲强度；

p ——理论光脉冲强度。

6.1.1.5 其他属性制备

其他属性制备检测的目的是检测各种量子态之间，在其他测量属性上均不可区分（如频域和时域属性等不可区分）。其他属性制备检测包括信号态下各种量子态幅度检测、诱骗态下各种量子态幅度检测、信号态与诱骗态下各种量子态脉宽检测、信号态与诱骗态下各种量子态光谱检测、信号态与诱骗态下各种量子态时间检测和相位随机化的检测。

各种量子态之间，在其他测量属性上应满足以下要求：

a) 信号态下，各种量子态之间幅度应满足：

$$\left|\frac{Amp_{\max}-Amp_{\min}}{Amp_{avg}}\right|<10\%$$

式中：

$Amp_{\max}$——幅度均方根最大值；

$Amp_{\min}$——幅度均方根最小值；

Amp_{avg}——幅度均方根平均值。

b) 诱骗态下，各种量子态之间幅度应满足：

$$\left|\frac{Amp_{\max}-Amp_{\min}}{Amp_{avg}}\right|<10\%$$

式中：

$Amp_{\max}$——幅度均方根最大值；

$Amp_{\min}$——幅度均方根最小值；

Amp_{avg}——幅度均方根平均值。

c) 信号态与诱骗态下，各种量子态之间脉宽均应满足：

$$|Wid_{\max}-Wid_{\min}|<20ps$$

式中：

$Wid_{\max}$——半高宽均方根最大值；

$Wid_{\min}$——半高宽均方根最小值。

d) 信号态与诱骗态下，各种量子态之间波长偏差和谱宽偏差均应小于 0.02 nm。

e) 信号态与诱骗态下，各种量子态之间相对参考时钟信号的时间偏差均应满足：

$$|Tim_{\max}-Tim_{\min}|<20ps$$

式中：

$Tim_{\max}$——时间偏差均方根最大值；

$Tim_{\min}$——时间偏差均方根最小值。

f) 若发送端使用脉冲光激光器制备光脉冲时，可不考虑相位随机化的要求；否则，发送方需在范围$[0,2\pi)$内对弱相干态光脉冲进行相位随机化操作，且选取的随机化相位数量不小于 10，并且取值应该均匀分布。

6.1.1.6 编码过程

编码过程检测的目的是检测发送端编码过程是否符合诱骗态 BB84 协议的要求。

编码即信息加载的过程，是发送端将用以加载信息的量子态随机加载在对应的光脉冲上，量子态可以是偏振、相位、自旋、时间、动量等。编码过程应符合 GM/T 0108—2021 的编码要求。

量子密钥分配产品在编码过程中，应至少具有抵御特洛伊木马攻击、激光注入攻击、种子光攻击的能力。抵御编码过程中的相关攻击可采用的推荐措施，见 GM/T 0108—2021 中附录 C 中 a)。

6.1.2 量子态传输过程检测

量子态传输过程检测的目的是检测量子态传输过程是否符合诱骗态 BB84 协议的要求。

发送端通过量子信道将符合 GM/T 0108—2021 中 6.2.1 要求的加载了信息的量子态的光脉冲发送给接收端，并记录所发光脉冲的光强制备信息和编码信息。

6.1.3 量子态测量过程检测

6.1.3.1 解码过程

解码过程检测的目的是检测接收端解码过程是否符合诱骗态 BB84 协议的要求。

解码过程是接收端随机选择一个测量基对发送端发来的加载了信息的量子态进行解调。应符合 GM/T 0108—2021 的解码要求。

在解码过程中，若接收端为主动选基方案时，应至少具有抵御特洛伊木马攻击的能力。

在解码过程中，若接收端为主动选基(不选态)时，应至少具有抵御荧光攻击的能力；若接收端为主动选基(不选态)且使用多个探测器时，应至少具有抵御伪造态攻击、时间位移攻击和设备校准攻击的能力。

在解码过程中，若接收端为被动选基方案时，应至少具有抵御波长相关攻击和抵御荧光攻击的能力；若接收端为被动选基方案且使用多个探测器时，应至少具有抵御伪造态攻击、时间位移攻击和设备校准攻击的能力。

抵御解码过程中的相关攻击可采用的推荐措施，见 GM/T 0108—2021 中附录 C 中 b)、c)、d)、e)、f)。

6.1.3.2 探测过程

探测过程检测包括接口检测、关键属性检测和防探测过程攻击检测，其检测目的分别是检测探测器的接口属性和关键属性是否符合诱骗态 BB84 协议的要求，是否采取抵御探测过程中的相关攻击的措施。

探测过程是对作为信息载体的单个光子的探测，将探测到的光脉冲的量子态信息转换成经典比特信息，得到原始密钥。目前的实现方式主要基于单光子探测器。

探测过程应符合 GM/T 0108—2021 中 6.2.3.2 的接口要求、关键属性要求和防攻击措施要求。抵御探测过程中的相关攻击可采用的推荐措施，见 GM/T 0108—2021 中附录 C 中 g)、h)、i)、j)、k)。

6.1.4 对基过程检测

对基过程是发送端和接收端将量子态制备时所采用的编码基与接收端所采用的测量基进行比对，双方只保留相同基矢的数据，生成筛后密钥。对基过程检测的目的是检测发送端和接收端的对基过程是否符合诱骗态 BB84 协议的要求。

对基过程应符合 GM/T 0108—2021 的对基过程的要求。

6.1.5 纠错过程检测

纠错过程是发送端和接收端纠正两端筛后密钥中的量子比特误码，获得一致的密钥，即纠错后密钥。纠错过程检测的目的是检测发送端和接收端的纠错过程是否符合诱骗态 BB84 协议的要求。

纠错过程应符合 GM/T 0108—2021 的纠错过程的要求。

6.1.6 安全增强过程检测

安全增强过程指发送端与接收端使用杂凑函数类对纠错后密钥进行杂凑，提取共享密钥的过程。安全增强过程检测的目的是检测发送端和接收端的安全增强过程是否符合诱骗态 BB84 协议的要求。

安全增强过程应符合 GM/T 0108—2021 的安全增强过程的要求。

6.2 量子密钥分配产品检测

6.2.1 基本检测

6.2.1.1 功能检测

量子密钥分配产品功能检测包括协议实现要求检测、共享密钥随机性检测和共享密钥一致性检测。协议实现要求检测的目的是检测量子密钥分配产品生成密钥的过程是否遵循诱骗态 BB84 协议。共享密钥随机性检测的目的是检测量子密钥分配产品生成密钥的随机性是否符合量子密钥分配产品的性能要求。共享密钥一致性的检测目的是检测量子密钥分配产品发送端和接收端生成的共享密钥是否一致。

量子密钥分配产品应遵循诱骗态 BB84 协议，应符合 GM/T 0108—2021 中 6.1 和 6.2 的要求。量子密钥分配产品产生的共享密钥的随机性应符合 GB/T 32915 的要求。量子密钥分配产品发送端和接收端产生的共享密钥应一致。

6.2.1.2 性能检测

6.2.1.2.1 共享密钥生成率

共享密钥生成率检测的目的是检测量子密钥分配产品在单位时间内生成的共享密钥量是否满足送检文档的规定。

量子密钥分配产品应符合产品送检文档中规定的共享密钥生成率的要求。

6.2.1.2.2 最大距离

量子密钥分配产品的最大距离检测的目的是检测量子密钥分配产品在满足性能和安全需求的前提下，发送端与接收端之间量子信道的最大长度。

量子密钥分配产品应符合产品送检文档中规定的最大距离的要求。

6.2.1.2.3 环境适应性和可靠性

环境适应性检测的目的是检测量子密钥分配产品对工作环境的适应性；可靠性检测的目的是检测量子密钥分配产品的平均无故障时间。

量子密钥分配产品的工作环境应根据实际需要符合 GB/T 2423.1 和 GB/T 2423.2 的要求。

量子密钥分配产品的可靠性应符合 GM/T 0108—2021 的可靠性的要求。

6.2.1.3 安全性设计检测

安全性设计检测的目的是检测量子密钥分配产品的安全性设计是否符合密码模块安全技术要求。

量子密钥分配产品的角色、服务和鉴别、物理安全、敏感安全参数管理及自测试等检测应符合 GB/T 37092 的要求。

6.2.2 鉴别检测

鉴别检测的目的是检测量子密钥分配产品的发送端与接收端之间，量子密钥分配产品与共享密钥管理层系统、管理平台或管理工具之间所采用的鉴别机制。

诱骗态 BB84 协议流程的对基和安全增强阶段，发送端与接收端之间通过经典信道交互的全部信息应采用消息鉴别，以保证信息完整性，鉴别机制应符合 GB/T 15852.1 或 GB/T 15852.2 或 GB/T 15852.3 的要求。

量子密钥分配产品的发送端与接收端之间应通过经典信道进行实体鉴别，以保证实体真实性，鉴别机制应符合 GB/T 15843.2 或 GB/T 15843.4 的要求。

量子密钥分配产品与共享密钥管理层系统、管理平台或管理工具之间也应通过经典信道进行实体鉴别，以保证实体真实性，鉴别机制应符合 GB/T 15843.2 或 GB/T 15843.4 的要求。他们之间交互的全部信息也应采用消息鉴别，鉴别机制应符合 GB/T 15852.1 或 GB/T 15852.2 或 GB/T 15852.3 的要求。

量子密钥分配产品的消息鉴别和实体鉴别机制所使用的密钥应事先预置；当所需密钥为对称密钥时，可采用由量子密钥分配产品自身产生的共享密钥进行替换。

量子密钥分配产品在鉴别过程中，应至少具备重放攻击的能力。

6.2.3 接口检测

接口检测的目的是检测量子密钥分配产品接口的类型和作用是否符合量子密钥分配产品的要求。

量子密钥分配产品的接口应符合 GM/T 0108—2021 的接口要求。

6.2.4 随机数发生器检测

随机数发生器检测的目的是检测量子密钥分配产品配用的随机数发生器的是否符合量子密钥分配产品的要求。

量子密钥分配产品配用的随机数发生器应取得国家密码管理部门的认可。

量子密钥分配产品配用的随机数发生器应使用基于物理过程的随机数发生器，并能通过送样检测、出厂检测、上电检测和使用检测四个不同应用阶段的随机数检测，应符合 GM/T 0062 中 D 类产品的要求。

6.2.5 日志管理检测

日志管理检测的目的是检测量子密钥分配产品对日志的管理是否符合量子密钥分配产品的要求。

量子密钥分配产品应提供日志功能，日志可被查看、导出。

日志内容包括：

a) 操作行为，包括登录认证、系统配置、密钥管理等操作；

b) 安全事件，包括与管理平台连接、密钥产生、密钥更新、密钥销毁等事件；

c) 异常事件，包括认证失败、非法访问、完整性校验失败等异常事件。

6.2.6 远程管理检测

远程管理检测的目的是检测量子密钥分配产品的远程管理功能是否符合量子密钥分配产品的要求。

量子密钥分配产品的远程管理应符合 GM/T 0108—2021 中 7.6 的要求。

7 检测方法

7.1 协议实现要求检测

7.1.1 基制备检测

7.1.1.1 编码基共轭性相对误差

以相位编码量子密钥分配产品的编码基共轭性相对误差检测为例：

——检测条件：

a) 虚线框部分应选择发送端基/态制备模块(含相位调制器)；

b) 光源的同步时钟信号应使得单光子探测器工作正常；

c) 应获得基/态制备模块调制 0、π/2、π、3π/2 的 4 个相位的调相电压 ϕ_0、ϕ_1、ϕ_2、ϕ_3；

d) 调整光源光功率至合适水平，使得到达单光子探测器的光脉冲的平均光子数水平与信号态光脉冲平均光子数水平一致，且至少保证单光子探测器探测计数应是单光子探测器暗计数的 2 倍以上。

——检测方法：

a) 按 5.2.1.1 中图 2 连接待测设备和陪测设备，设置激光器触发频率为 n MHz，相位调制频率为 $2n$ MHz。利用光学和电子学延时技术使得，进入基/态制备模块后第一次被加载相位的量子光与从末端反射镜反射回来被加载相位的量子光在进环形器前进行干涉；测量所需的干涉峰位置应在单光子探测器的探测门宽范围以内。

b) 光源发光并分别按照下列相位调制方式调制，并获取计数值：对离开基/态制备模块的量子光加载调相电压 ϕ_0，对返回基/态制备模块的量子光加载调相电压 ϕ_0，此时记录计数率为 S_{00}；对离开基/态制备模块的量子光加载调相电压 ϕ_0，对返回基/态制备模块的量子光加载调相电压 ϕ_1，此时记录计数率为 S_{01}，对离开基/态制备模块的量子光加载调相电压 ϕ_1，对返回基/态制备模块的量子光加载调相电压 ϕ_3，此时记录计数率为 S_{13}；对离开基/态制备模块的量子光加载调相电压 ϕ_0，对返回基/态制备模块的量子光加载调相电压 ϕ_2，此时记录计数率为 S_{02}；计数率为“每秒探测计数/探测器工作频率”。

c) 根据量子光学理论，由下述公式计算干涉光强 μ'_{00}，μ'_{01}，μ'_{13}，μ'_{02}。$S_{00}=1-(1-d)e^{-\eta\mu'_{00}}$，$S_{02}=1-(1-d)e^{-\eta\mu'_{02}}$，$S_{13}=1-(1-d)e^{-\eta\mu'_{13}}$，$S_{01}=1-(1-d)e^{-\eta\mu'_{01}}$，其中 d 为单光子探测器的暗计数率，η 为信道总效率，单光子探测器量子效率等因素决定信道总效率。

d) 设 $\phi'_0=0$，由下述公式进一步计算相位差 ϕ'_1，ϕ'_2，ϕ'_3：

$$\phi'_1=2\arccos\left(\sqrt{\frac{\mu'_{01}}{\mu'_{00}}}\right),\ \phi'_2=2\arccos\left(\sqrt{\frac{\mu'_{02}}{\mu'_{00}}}\right),\ \phi'_3=\phi_1-2\arccos\left(\sqrt{\frac{\mu'_{13}}{\mu'_{00}}}\right)+2\pi。$$

e) $A=|\langle\phi_1|\Psi_1\rangle|=\left|\cos\frac{\phi'_1-\phi'_0}{2}\right|$，$B=\left|\cos\frac{\phi'_3-\phi'_0}{2}\right|$，$C=\left|\cos\frac{\phi'_2-\phi'_1}{2}\right|$，$D=\left|\cos\frac{\phi'_3-\phi'_2}{2}\right|$，计算出最大共轭误差 $\sum=\mathrm{Max}(|A-E|,|B-E|,|C-E|,|D-E|)$；

f) 根据 6.1.1.2 的定义，得出共轭性相对误差 $\frac{\sum}{E}$。

——通过标准：编码基共轭性相对误差应符合 6.1.1.2 的要求。

以偏振编码量子密钥分配产品的编码基共轭性相对误差检测为例：

——检测方法：

a) 按 5.2.1.1 中图 3 连接待测待测设备和陪测设备，发送端通过光纤连接到偏振分析仪；

b) 控制发送端发送周期光“信号态 SH”(即 $|H\rangle$ 偏振态)，使用偏振分析仪记录当前偏振位

置 a，设 $\phi_0=0$；

c) 控制发送端发送周期光“信号态 SV”（即$|V\rangle$偏振态），使用偏振分析仪记录当前偏振位置 b，记录偏振位置 b 与 a 的夹角 ϕ_2；

d) 控制发送端发送周期光“信号态 SP”（即$|P\rangle$偏振态），使用偏振分析仪记录当前偏振位置 c；记录偏振位置 c 与 a 的夹角 ϕ_1；

e) 控制发送端发送周期光“信号态 SN”（即$|N\rangle$偏振态），使用偏振分析仪记录当前偏振位置 d；记录偏振位置 d 与 a 的夹角 ϕ_3；

f) $A=|\langle\varphi_1|\Psi_1\rangle|=|\cos(\phi_1-\phi_0)|$，$B=|\cos(\phi_3-\phi_0)|$，$C=|\cos(\phi_2-\phi_1)|$，$D=|\cos(\phi_3-\phi_2)|$，计算出最大共轭误差$\sum=\mathrm{Max}(|A-E|,|B-E|,|C-E|,|D-E|)$；

g) 根据 6.1.1.2 的定义，得出共轭性相对误差$\frac{\sum}{E}$。

——通过标准：编码基共轭性相对误差应符合 6.1.1.2 的要求。

7.1.1.2 测量基共轭性相对误差

以相位编码量子密钥分配产品的测量基共轭性相对误差检测为例：

——检测条件：

a) 虚线框部分选择接收端量子态解调模块（含相位调制器）；

b) 光源的同步时钟信号使得单光子探测器工作正常；

c) 应获得量子态解调模块调制 0、π/2、π、3π/2 的 4 个相位的调相电压 ϕ_0、ϕ_1、ϕ_2、ϕ_3；

d) 调整光源光功率至一合适水平，使得到达单光子探测器的光脉冲的平均光子数与信号态光脉冲平均光子数一致，且至少保证单光子探测器探测计数应是单光子探测器暗计数的 2 倍以上。

——检测方法：按 5.2.1.1 中图 4 连接待测设备和陪测设备，操作步骤同 7.1.1.1 检测方法步骤 a)～g)，得出共轭性相对误差$\frac{\sum}{E}$。

——通过标准：测量基共轭性相对误差应符合 6.1.1.2 的要求。

以偏振编码量子密钥分配产品的测量基相对误差检测为例：

——检测方法：

a) 按 5.2.1.1 中图 5 连接待测设备和陪测设备；

b) 将两个光功率计分别接入$|H\rangle$、$|V\rangle$偏振态输出端，调节发送端基/态制备模块，使接入$|H\rangle$偏振态输出端光功率计与接入$|V\rangle$偏振态输出端光功率计的读数比值最大，将偏振分析仪与$|H\rangle$偏振态输出端连接，记录当前偏振位置 a，设 $\phi_0=0$；

c) 将两个光功率计分别接入$|H\rangle$、$|V\rangle$偏振态输出端，调节发送端基/态制备模块，使接入$|H\rangle$偏振态输出端光功率计与接入$|V\rangle$偏振态输出端光功率计的读数比值最小，将偏振分析仪与$|V\rangle$偏振态输出端连接，记录当前偏振位置 b，记录偏振位置 b 与 a 的夹角 ϕ_2；

d) 将两个光功率计分别接入$|P\rangle$、$|N\rangle$偏振态输出端，调节发送端基/态制备模块，使接入$|P\rangle$偏振态输出端光功率计与接入$|N\rangle$偏振态输出端光功率计的读数比值最大，将偏振分析仪与$|P\rangle$偏振态输出端连接，记录当前偏振位置 c，记录偏振位置 c 与 a 的夹角 ϕ_1；

e) 将两个光功率计分别接入$|P\rangle$、$|N\rangle$偏振态输出端，调节发送端基/态制备模块，使接入$|P\rangle$偏振态输出端光功率计与接入$|N\rangle$偏振态输出端光功率计的读数比值最小，将偏振分析仪与$|N\rangle$偏振态输出端连接，记录当前偏振位置 d，记录偏振位置 d 与 a 的夹角 ϕ_3；

f) $A=|\langle\varphi_1|\Psi_1\rangle|=|\cos(\phi_1-\phi_0)|$，$B=|\cos(\phi_3-\phi_0)|$，$C=|\cos(\phi_2-\phi_1)|$，$D=|\cos(\phi_3-\phi_2)|$，计算出最大共轭误差$\sum=\mathrm{Max}(|A-E|,|B-E|,|C-E|,|D-E|)$；

g) 根据 6.1.1.2 的定义，得出共轭性相对误差$\frac{\sum}{E}$。

——通过标准：测量基共轭性相对误差应符合 6.1.1.2 的要求。

7.1.1.3 编码基与测量基的相对误差

以相位编码量子密钥分配产品的编码基与测量基的相对误差检测为例：

——检测条件：

a) 量子密钥分配产品具有生成和导出运行过程中各编解码状态下的探测计数矩阵的功能；

b) 应保证信号态探测器计数矩阵中最大计数值大于 10^5。

——检测方法：

a) 按 5.2.1.1 中图 6 连接待测设备和陪测设备，导出运行过程中各编解码状态下的信号态探测计数矩阵和光源不发光时的探测器计数矩阵，矩阵中各位置的计数见表 1、表 2：

表 1 信号态探测计数矩阵

信号态探测计数矩阵		发送端				
		编码基	Φ		Ψ	
接收端	测量基	态	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\Psi_1\rangle$	$\|\Psi_2\rangle$
	Φ	$\|\varphi_1\rangle$	S_{00}	S_{01}	S_{02}	S_{03}
		$\|\varphi_2\rangle$	S_{10}	S_{11}	S_{12}	S_{13}
	Ψ	$\|\Psi_1\rangle$	S_{20}	S_{21}	S_{22}	S_{23}
		$\|\Psi_2\rangle$	S_{30}	S_{31}	S_{32}	S_{33}

表 2 光源不发光时的探测计数矩阵

光源不发光时的探测计数矩阵		发送端				
		编码基	Φ		Ψ	
接收端	测量基	态	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\Psi_1\rangle$	$\|\Psi_2\rangle$
	Φ	$\|\varphi_1\rangle$	D_{00}	D_{01}	D_{02}	D_{03}
		$\|\varphi_2\rangle$	D_{10}	D_{11}	D_{12}	D_{13}
	Ψ	$\|\Psi_1\rangle$	D_{20}	D_{21}	D_{22}	D_{23}
		$\|\Psi_2\rangle$	D_{30}	D_{31}	D_{32}	D_{33}

b) 使用光源不发光时的总探测计数，即探测器暗计数 $D=\sum_{i=0}^{3}\sum_{j=0}^{3}D_{ij}$，$i$ 和 j 分别代表矩阵中的行号和列号，i、$j=0,1,2,3$；

c) 将送检产品的选基比例设计：$n:m$（若平衡选基，则 $n:m=1:1$）及矩阵中对应位置的探测计数值带入公式 $\delta\theta_{\max}=\frac{2}{\pi}\max\{\delta\theta_{bbk},\{b\in\{\Phi,\Psi\},k\in\{\phi_1,\phi_2,\Psi_1,\Psi_2\}\}\}$，计算编码基与测量基的相对误差；

d) 其中 $\delta\theta_{bbk}$ 的计算公式如下：

$$\delta\theta_{\Phi\Phi|\phi1\rangle}=\arcsin\sqrt{\frac{S_{10}-\frac{n^2}{4(n+m)^2}D}{S_{00}+S_{10}-\frac{n^2}{4(n+m)^2}(D+D)}},$$

$$\delta\theta_{\Phi\Phi|\phi_2\rangle}=\arcsin\sqrt{\frac{S_{01}-\frac{n^2}{4(n+m)^2}D}{S_{11}+S_{01}-\frac{n^2}{4(n+m)^2}(D+D)}},$$

$$\delta\theta_{\Psi\Psi|\Psi_1\rangle}=\arcsin\sqrt{\frac{S_{32}-\frac{m^2}{4(m+n)^2}D}{S_{22}+S_{32}-\frac{m^2}{4(m+n)^2}(D+D)}},$$

$$\delta\theta_{\Psi\Psi|\Psi_2\rangle}=\arcsin\sqrt{\frac{S_{23}-\frac{m^2}{4(m+n)^2}D}{S_{33}+S_{23}-\frac{m^2}{4(m+n)^2}(D+D)}}。$$

——通过标准：编码基与测量基的相对误差应符合 6.1.1.2 的要求。

以偏振编码量子密钥分配产品的编码基与测量基的相对误差检测为例：

——检测条件：

a) 量子密钥分配产品具有生成和导出运行过程中各编解码状态下的探测计数矩阵的功能；

b) 应保证信号态探测器计数矩阵中最大计数值大于 10^5；

——检测方法：

a) 按 5.2.1.1 中图 6 连接待测设备和陪测设备，导出运行过程中各编解码和真空状态下的计数矩阵，矩阵中各位置的计数见表 3；

表 3 探测计数矩阵

探测计数矩阵		发送端					Vaccum
		编码基	Φ		Ψ		
接收端	测量基	态	$\|\varphi_1\rangle$	$\|\varphi_2\rangle$	$\|\Psi_1\rangle$	$\|\Psi_2\rangle$	
	Φ	$\|\varphi_1\rangle$	S_{00}	S_{01}	S_{02}	S_{03}	D_0
		$\|\varphi_2\rangle$	S_{10}	S_{11}	S_{12}	S_{13}	D_1
	Ψ	$\|\Psi_1\rangle$	S_{20}	S_{21}	S_{22}	S_{23}	D_2
		$\|\Psi_2\rangle$	S_{30}	S_{31}	S_{32}	S_{33}	D_3

b) 用真空态发送总数除计数，计算出探测器每发送脉冲的总暗计数率 $d=\frac{\sum_{i=0}^{3}D_i}{N_{\text{vaccum}}}$，对于多探测器方案，可以对每个通道的探测器分别计算暗计数率 $d_i=\frac{D_i}{N_{\text{vaccum}}}$；

c) 根据公式 $\delta\theta_{\max}=\frac{2}{\pi}\max\{\delta\theta_{bbk},\{b\in\{\Phi,\Psi\},k\in\{\phi_1,\phi_2,\Psi_1,\Psi_2\}\}\}$，计算编码基与测量基的相对误差；

d) 其中，N_{sys}为系统发送脉冲总数，为系统频率 * 时间；P_μ、P_ν为诱骗态方案设置的信号态、诱骗态、真空态的制备概率；分别表示发送端的信号态的 Φ/Ψ 基制备概率、发送端的诱骗态的 Φ/Ψ 基制备概率、接收端的 Φ/Ψ 基制备概率；为发送端的 Φ 基、Ψ 基下，态的制备概率，平衡时默认为 1/2。

$$\delta\theta_{\Phi\Phi|\phi_1\rangle}=\arcsin\sqrt{\frac{S_{10}-N_{\Phi\Phi|\phi_1\rangle}d_1}{S_{00}+S_{10}-N_{\Phi\Phi|\phi_1\rangle}(d_0+d_1)}},$$

$$\delta\theta_{\Phi\Phi|\phi_2\rangle}=\arcsin\sqrt{\frac{S_{01}-N_{\Phi\Phi|\phi_2\rangle}d_0}{S_{11}+S_{01}-N_{\Phi\Phi|\phi_2\rangle}(d_0+d_1)}},$$

$$\delta\theta_{\Psi\Psi|\Psi_1\rangle}=\arcsin\sqrt{\frac{S_{32}-N_{\Psi\Psi|\Psi_1\rangle}d_3}{S_{22}+S_{32}-N_{\Psi\Psi|\Psi_1\rangle}(d_2+d_3)}},$$

$$\delta\theta_{\Psi\Psi|\Psi_2\rangle}=\arcsin\sqrt{\frac{S_{23}-N_{\Psi\Psi|\Psi_2\rangle}d_2}{S_{33}+S_{23}-N_{\Psi\Psi|\Psi_2\rangle}(d_3+d_2)}},$$

$$N_{\Phi\Phi|\phi_1\rangle}=N_{sys}*(P_\mu*q_{a\mu\Phi}+P_\nu*q_{a\nu\Phi})*\rho_{a\Phi|\phi_1\rangle}*q_{b\Phi},$$

$$N_{\Phi\Phi|\phi_2\rangle}=N_{sys}*(P_\mu*q_{a\mu\Phi}+P_\nu*q_{a\nu\Phi})*\rho_{a\Phi|\phi_2\rangle}*q_{b\Phi},$$

$$N_{\Psi\Psi|\Psi_1\rangle}=N_{sys}*(P_\mu*q_{a\mu\Psi}+P_\nu*q_{a\nu\Psi})*\rho_{a\Psi|\Psi_1\rangle}*q_{b\Psi},$$

$$N_{\Psi\Psi|\Psi_2\rangle}=N_{sys}*(P_\mu*q_{a\mu\Psi}+P_\nu*q_{a\nu\Psi})*\rho_{a\Psi|\Psi_2\rangle}*q_{b\Psi}。$$

——通过标准：编码基与测量基的相对误差应符合 6.1.1.2 的要求。

7.1.2 态制备检测

以相位编码量子密钥分配产品的态制备误差检测为例：

——检测条件：同 7.1.1.1、7.1.1.2 相位编码量子密钥分配产品检测条件。

——检测方法：

a) 同 7.1.1.1、7.1.1.2 相位编码量子密钥分配产品的编码基共轭性相对误差和测量基共轭性相对误差的检测方法，得出 ϕ_1'，ϕ_2'，ϕ_3'相位；

b) $\theta_X=\arccos|\langle\varphi_1|\varphi_2\rangle|=\arccos\left|\cos\frac{\phi_2'-\phi_0'}{2}\right|$，$\theta_Y=\arccos|\langle\Psi_1|\Psi_2\rangle|=\arccos\left|\cos\frac{\phi_3'-\phi_1'}{2}\right|$，计算出正交误差。

——通过标准：每组基的两种量子态应正交，正交误差应符合 6.1.1.3 的要求。

以偏振编码量子密钥分配产品的态制备误差检测为例：

——检测条件：同 7.1.1.1、7.1.1.2 偏振编码量子密钥分配产品检测条件。

——检测方法：

a) 同 7.1.1.1、7.1.1.2 偏振编码量子密钥分配产品的编码基共轭性相对误差和测量基共轭性相对误差的检测方法，得出 ϕ_1，ϕ_2，ϕ_3的夹角；

b) $\theta_X=\arccos|\langle\varphi_1|\varphi_2\rangle|=\arccos|\cos(\phi_2-\phi_0)|$，$\theta_Y=\arccos|\langle\Psi_1|\Psi_2\rangle|=\arccos|\cos(\phi_3-\phi_1)|$，计算出正交误差。

——通过标准：每组基的两种量子态应正交，正交误差应符合 6.1.1.3 的要求。

7.1.3 光强制备检测

——检测条件：

a) 量子密钥分配产品应具备单独制备信号态和诱骗态 1、诱骗态 2 的模式；

b) 量子密钥分配产品可能工作于光强扫描模式，检测时需对扫描模式和工作模式进行区分；

c) 对于量子光和同步光合波输出情况，可使用高隔离度波分复用器分离同步光，功率测量只考虑器件插损的影响；

d) 光功率计灵敏度不满足要求时，可将发送端内部衰减值减小至光功率计可正常检测的范围，最终计算时扣除减小的衰减值。

——检测方法：

a) 按 5.2.1.2 中图 7 连接待测设备和陪测设备，依次设置发送端按照标准工作模式的强度，输出信号态的光脉冲、诱骗态 1 的光脉冲、诱骗态 2 的光脉冲；

b) 使用光功率计测量发送端的输出光功率，光强统计的时间间隔不小于 1 s，采样点数不小

于 100，对采集到的光功率测量值取均方根作为实际光脉冲强度 p'；

c) 计算理论光脉冲强度，以信号态为例：测得信号态光脉冲重复频率为 f，信号态光脉冲中心波长为 λ，理论平均光子数为 μ，单光子能量为 $E_p=h\cdot\frac{c}{\lambda}$，可得理论光脉冲强度为 $p=\mu\cdot E_p$，其中 h 为普朗克常量，c 为光速。

——通过标准：

光强度制备符合 6.1.1.4 的要求。

7.1.4 其他属性制备检测

7.1.4.1 信号态下各种量子态幅度

——检测条件：量子密钥分配产品应具备单独制备信号态的模式。

——检测方法：

a) 按 5.2.1.3 中图 8 连接待测设备和陪测设备，设置发送端按照标准工作模式的强度，输出信号态的光脉冲；

b) 使用示波器自带的脉冲幅度测量工具对光脉冲幅度进行测量，并统计光脉冲幅度的均方根值；

c) 设置输出不同量子态的光脉冲，依次对每个量子态的光脉冲幅度进行测量，统计出每种量子态光脉冲幅度的均方根值；

d) 当发送端输出的光强低于测量设备的测量范围时，可减小发送端内部光路衰减，以使发送端输出光强达到测量要求。

——通过标准：检测结果应符合 6.1.1.5 的要求。

7.1.4.2 诱骗态下各种量子态幅度

——检测条件：量子密钥分配产品应具备单独制备诱骗态的模式。

——检测方法：

a) 按 5.2.1.3 中图 8 连接待测设备和陪测设备，设置发送端按照标准工作模式的强度，输出诱骗态的光脉冲；

b) 使用示波器自带的脉冲幅度测量工具对光脉冲幅度进行测量，并统计光脉冲幅度的均方根值；

c) 设置输出不同量子态的光脉冲，依次对每个量子态的光脉冲幅度进行测量，统计出每种量子态光脉冲幅度的均方根值；

d) 当发送端输出的光强低于测量设备的测量范围时，可减小发送端内部光路衰减，以使发送端输出光强达到测量要求。

——通过标准：检测结果应符合 6.1.1.5 的要求。

7.1.4.3 信号态与诱骗态下各种量子态脉宽

——检测方法：

a) 按 5.2.1.3 中图 8 连接待测设备和陪测设备；

b) 使用示波器自带的脉冲宽度测量工具对光脉冲宽度进行测量，并统计光脉冲宽度的均方根值；

c) 设置光源输出不同量子态的光脉冲，依次对每个量子态的光脉冲宽度进行测量，统计出每种量子态态光脉冲宽度的均方根值；

d) 当发送端输出的光强低于测量设备的测量范围时，可减小发送端内部光路衰减，以使发

送端输出光强达到测量要求。

——通过标准：检测结果应符合 6.1.1.5 的要求。

7.1.4.4 信号态与诱骗态下各种量子态光谱

——检测方法：

a) 按 5.2.1.3 中图 9 连接待测设备和陪测设备；

b) 使用光谱分析仪测量光脉冲的－3 dB 中心波长和－3 dB 光谱宽度；

c) 设置光源输出不同量子态的光脉冲，依次对每个量子态的光脉冲的－3 dB 中心波长和－3 dB 光谱宽度进行测量，统计出每种量子态光脉冲－3 dB 中心波长和－3 dB 光谱宽度；

d) 当发送端输出的光强低于测量设备的测量范围时，可减小发送端内部光路衰减，以使发送端输出光强达到测量要求。

——通过标准：检测结果应符合 6.1.1.5 的要求。

7.1.4.5 信号态与诱骗态下各种量子态时间

——检测方法：

a) 按 5.2.1.3 中图 10 连接待测设备和陪测设备；

b) 示波器以参考时钟信号进行触发，使用示波器自带的时延测量工具，测量光脉冲峰值中心位置相对参考时钟信号的特定位置的时间偏差，并统计光脉冲时间偏差的均方根值；

c) 设置光源输出不同量子态的光脉冲，依次对每个量子态的光脉冲相对参考时钟信号的特定位置的时间偏差进行测量，统计出每种量子态光脉冲时间偏差的均方根值；

d) 当发送端输出的光强低于测量设备的测量范围时，可减小发送端内部光路衰减，以使发送端输出光强达到测量要求。

——通过标准：检测结果应符合 6.1.1.5 的要求。

7.1.4.6 相位随机化

——检测条件：厂商应提供相关设计文档以供审查。

——检测方法：

a) 通过文档审查的方式核实待测量子密钥分配产品发送端是否是使用脉冲光激光器制备光脉冲；

b) 若发送端非使用脉冲光激光器制备光脉冲，则是否具备相位随机化的装置对光脉冲进行相位随机化操作。

——通过标准：检测结果应符合 6.1.1.5 的要求。

7.1.5 编码过程检测

——检测条件：厂商应提供相关设计文档以供审查。

——检测方法：通过文档审查和代码审查的方式，检测待测量子密钥分配产品的编码过程是否符合 GM/T 0108—2021 中编码过程的要求。并对发送端将用以加载信息的量子态随机加载在对应的光脉冲上所采用的随机数进行随机性检测。防编码过程攻击检测的方法见 7.2.1。

——通过标准：检测结果应符合 GM/T 0108—2021 的编码要求。

7.1.6 量子态传输过程检测

——检测条件：厂商应提供相关设计文档以供审查。

——检测方法：通过文档审查和代码审查的方式，检测待测产品的编码过程是否符合 GM/T 0108—2021 量子态传输过程的要求。

——通过标准：检测结果应符合 GM/T 0108—2021 的量子态传输过程要求。

7.1.7 解码过程检测

——检测条件：厂商应提供相关设计文档以供审查。

——检测方法：通过文档审查和代码审查的方式，检测待测产品的解码过程是否符合 GM/T 0108—2021 中解码过程的要求。并对接收端用以选择测量基的随机数进行随机性检测。防解码过程攻击检测的方法见 7.2.2。

——通过标准：检测结果应符合 GM/T 0108—2021 的解码要求。

7.1.8 探测器接口检测

——检测方法：对探测器接口类型和接口功能进行检测。

——通过标准：检测结果应符合 6.1.3.2 的接口要求。

7.1.9 探测器关键属性检测

7.1.9.1 探测效率半高宽

——检测条件：

a) 探测器工作频率 f_g 和窄脉冲光源脉冲重复频率 f_p 满足整除关系；

b) 光脉冲宽度应小于探测器的门控宽度；

c) 信号源两路通道的输出信号重复频率应能够分别与探测器工作频率和窄脉冲光源重复频率匹配，且有输出延时扫描功能。

——检测方法：

a) 按 5.2.1.4 中图 11 连接待测探测器和测量设备，模拟探测器实际使用场景，输出特定频率特定强度的单光子光脉冲，即得到单位时间输入被测探测器的光子数；

b) 输出光频整数倍的周期门控信号给探测器；调节信号源两路通道的相对延时，即对门控信号和光脉冲信号的相对延时位置进行扫描，记录每个相对时间位置的探测器计数率；

c) 扫描时间范围大于等于一个门控信号周期，根据探测计数率扫描数据绘制得到被测探测器的探测效率曲线，同时得到效率曲线半高宽；

d) 重复上述步骤，依次测量得到接收端每个通道探测器的探测效率曲线及其半高宽。

——通过标准：探测效率半高宽应符合 6.1.3.2 关键属性要求。

7.1.9.2 探测效率峰值

——检测条件：

a) 探测器工作频率 f_g 和窄脉冲光源脉冲重复频率 f_p 满足整除关系；

b) 光脉冲宽度应小于探测器的门控宽度；

c) 信号源两路通道的输出信号重复频率应能够分别与探测器工作频率和窄脉冲光源重复频率匹配，且有输出延时扫描功能。

——检测方法：

a) 按 5.2.1.4 中图 11 连接待测探测器模块和测量设备，模拟探测器实际使用场景，在不发光情况下，测量得到被测探测器的单位时间暗计数；

b) 模拟探测器实际使用场景，输出特定频率特定强度的单光子脉冲，即使得光脉冲强度为 μ

光子/脉冲，同时输出光频整数倍的周期门控信号给探测器；

c) 调节信号源两路通道相对延时，即进行门控信号与光脉冲信号的相对延时位置扫描，找到探测计数最大位置，得到最大单位时间探测计数，根据探测效率计算公式计算得到被测探测器的探测效率峰值；

d) 探测效率计算公式如下：

$$\eta=\frac{N}{\mu}\ln\left(\frac{1-\frac{R_{dc}}{f_g}}{1-\frac{R_{de}}{f_g}}\right)$$

式中：

μ ——光脉冲的平均光子数；

η ——探测效率；

R_{dc} ——单位时间暗计数；

R_{de} ——单位时间探测计数；

f_p ——光源脉冲重复频率；

f_g ——探测器工作频率；

N ——$\frac{f_g}{f_p}$。

e) 重复上述步骤，依次测量得到每个通道探测器的探测效率峰值。

——通过标准：探测效率半高宽应符合 6.1.3.2 关键属性要求。

7.1.10 对基过程检测

——检测条件：

a) 厂商提供对基过程的协议设计方案；

b) 量子密钥分配产品具有导出对基过程前后相关数据的检测接口。

——检测方法：

a) 按 5.2.1.6 中图 15 连接待测设备和陪测设备，通过在经典信道抓取数据包的方式，提取对基过程的标识字段，并与厂商提供的协议设计方案进行比对是否一致；

b) 在对基前数据相同的情况下，比对离线对基后的数据与量子密钥分配产品自身执行对基后的数据的一致性，检测待测量子密钥分配产品执行对基过程的正确性；

c) 通过文档审查和数据经典信道抓取数据包的方式，检测对基过程中发送端与接收端之间通过经典信道交互的全部信息是否有鉴别过程，并且鉴别过程符合 GM/T 0108—2021 所规定的鉴别的要求；

d) 依据 a)、b)检测结果，通过文档审查和代码审查的方式，检测待测量子密钥分配产品的对基过程是否符合 GM/T 0108—2021 的对基过程的要求。

——通过标准：检测结果应符合 GM/T 0108—2021 的对基过程的要求。

7.1.11 纠错过程检测

——检测条件：

a) 厂商提供纠错过程的协议设计方案；

b) 量子密钥分配产品具有导出纠错前后数据的检测接口。

——检测方法：

a) 按 5.2.1.6 中图 15 连接待测设备和陪测设备，通过在经典信道抓取数据包的方式，提取纠

错过程的标识字段，并与厂商提供的协议设计方案进行比对是否一致；

b) 在纠错前数据相同的情况下，比对离线纠错后的数据与量子密钥分配产品自身执行纠错后的数据的一致性，检测量子密钥分配产品执行纠错过程的正确性；

c) 依据 a)、b)检测结果，通过文档审查和代码审查的方式，检测待测量子密钥分配产品的纠错过程是否符合 GM/T 0108—2021 的纠错过程的要求。

——通过标准：检测结果应符合 GM/T 0108—2021 的纠错过程的要求。

7.1.12 安全增强过程检测

——检测条件：

a) 厂商提供安全增强过程的协议设计方案；

b) 产品具有导出安全增强前后数据的检测接口。

——检测方法：

a) 按 5.2.1.6 中图 15 连接待测设备和陪测设备，通过在经典信道抓取数据包的方式，提取安全增强过程的标识字段，并与厂商提供的协议设计方案进行比对是否一致；

b) 在安全增强前数据相同的情况下，比对离线安全增强后的数据与量子密钥分配产品自身执行安全增强后的数据的一致性，检测量子密钥分配产品执行安全增强过程的正确性；

c) 通过文档审查及代码走查的方式，检测安全增强过程中的压缩比 R 的计算方法是否符合 GM/T 0108—2021 中的附录 E 的要求；

d) 通过文档审查和数据经典信道抓取数据包的方式，检测安全增强过程中发送端与接收端之间通过经典信道交互的全部信息是否有鉴别过程，并且鉴别过程符合 GM/T 0108—2021 所规定的鉴别的要求；

e) 根据 a)、b)、c)、d)的检测结果，通过文档审查和代码审查的方式，检测待测量子密钥分配产品的安全增强过程是否符合 GM/T 0108—2021 的安全增强过程的要求。

——通过标准：检测结果应符合 GM/T 0108—2021 的安全增强过程的要求。

7.2 防攻击检测

7.2.1 防编码过程攻击检测

7.2.1.1 特洛伊木马攻击防护

——检测条件：发送端编码模块输出位置应预留测试接口。

——检测方法：

a) 测试从发送端出口至编码模块入口处的线路衰减，记为 a；

b) 测试从编码模块入口至发送端出口处的线路衰减，记为 b。

——通过标准：a 与 b 的衰减之和应不小于 110 dB。

7.2.1.2 激光注入攻击防护

检测方法：见 7.2.1.1。

7.2.1.3 种子光注入攻击防护

检测方法：见 7.2.1.1。

7.2.2 防解码过程攻击检测

7.2.2.1 特洛伊木马攻击防护

——检测条件：接收端编码模块输出位置应预留测试接口。

——检测方法：

a） 测试从接收端入口至编码模块出口处的线路衰减，记为 a；

b） 测试从解码模块出口至接收端入口处的线路衰减，记为 b。

c） 结合强光致盲告警阈值 $P_{warning}$，可得接收端回波功率的下限 $P=P_{warning}-|a+b|$。

——通过标准：P 应不大于−95 dBm。

注：接收端为主动选基方案时，应做特洛伊木马攻击防护的相关检测。

7.2.2.2 波长相关攻击防护

——检测条件：接收端解码模块的基矢选择器件（分束器）应预留测试接口。

——检测方法：测试在不同输入光波长的情况下，基矢选择器件的光脉冲强度分束比。

——通过标准：在不同输入光波长的情况下，基矢选择器件的光脉冲强度分束比应一致。

注：接收端为被动选基方案时，应做波长相关攻击防护的相关检测。

7.2.2.3 荧光攻击防护

检测方法：见 7.2.2.1。

注：接收端为主动选基（不选态），或接收端为被动选基方案时，应做荧光攻击防护的相关检测。

7.2.2.4 伪造态攻击防护

检测方法：见 7.1.9.1、7.1.9.2。

注：接收端为主动选基（不选态）且使用多个探测器，或接收端为被动选基方案且使用多个探测器时，应做伪造态攻击防护的相关检测。

7.2.2.5 时间位移攻击防护

检测方法：见 7.1.9.1、7.1.9.2。

注：接收端为主动选基（不选态）且使用多个探测器，或接收端为被动选基方案且使用多个探测器时，应做时间位移攻击防护的相关检测。

7.2.2.6 设备校准攻击防护

——检测方法：

a） 按 5.2.1.5 中图 14 连接待测单光子探测器以及测量设备，调节量子密钥分配产品至正常运行；

b） 在量子密钥分配产品延时校准过程中，施加设定好的可造成被测探测器效率曲线偏移的伪态强光；

c） 观察探测器的延时扫描结果是否在给定的阈值范围内，检测量子密钥分配产品是否在受到攻击时，发现异常并进行告警。

——通过标准：量子密钥分配产品在探测器受到设备校准攻击时发出告警。

注：接收端为主动选基（不选态）且使用多个探测器，或接收端为被动选基方案且使用多个探测器时，应做设备校准攻击防护的相关检测。

7.2.3 防探测过程攻击检测

7.2.3.1 强光攻击防护

——检测条件：

a） 连续波光源接入光源合束器前，应确保输出光强已衰减至不影响量子密钥分配产品正常

运行参数的强度；

b） 若量子密钥分配产品可实时统计探测器的探测计数并显示或输出，则可不用脉冲计数器对探测计数进行统计。

——检测方法：

a） 按 5.2.1.5 中图 12 连接待测单光子探测器以及测量设备，调节量子密钥分配产品至正常运行；

b） 逐渐增强连续波光源的输出光强，脉冲计数器计数随之增长；

c） 检测量子密钥分配产品是否在探测器被致盲（脉冲计数器的计数值下降为 0）前，发现强光攻击的异常，并进行告警。

——通过标准：量子密钥分配产品在探测器被致盲前检测出受到强光攻击并发出告警。

注：接收端使用基于 APD 的单光子探测器时，应做单光子探测器强光攻击防护的相关检测。

7.2.3.2 双计数攻击防护

——检测方法：

a） 按 5.2.1.5 中图 13 连接待测单光子探测器以及测量设备；

b） 正常运行被测探测器的所在的量子密钥分配产品，在量子密钥分配产品正常运行过程中，施加设定好的攻击脉冲，使探测器能够较大概率出现双计数现象；

c） 检测量子密钥分配产品是否在受到双计数攻击时，发现异常并告警；

d） 也通过审查送检文档的方式进行该项检测。

——通过标准：量子密钥分配产品在探测器受到双计数攻击时，自动对同一基下的双探测器响应事件应使用随机赋值方式处理，对不同基下的双探测器响应事件应直接丢弃。

注：接收端使用多个单光子探测器时，应做单光子探测器双计数攻击防护的相关检测。

7.2.3.3 波长相关性攻击防护

——检测条件：

a） 单光子探测器工作频率 f_g 和波长可调节的窄脉冲光源脉冲重复频率 f_p 满足整除关系；

b） 光脉冲宽度应小于单光子探测器的门控宽度；

c） 信号源重复频率能够和单光子探测器工作频率匹配；具有双通道且有输出延时扫描功能。

——检测方法：

a） 按 5.2.1.4 中图 11 连接待测探测器模块和测量设备，模拟探测器实际使用场景，在不发光情况下，测量得到被测探测器的单位时间暗计数；

b） 模拟探测器实际使用场景，输出特定频率特定强度的单光子脉冲，即使得光脉冲强度为 μ 光子/脉冲，同时输出光频整数倍的周期门控信号给探测器；

c） 调节信号源两路通道相对延时，即进行门控信号与光脉冲信号的相对延时位置扫描，找到探测计数最大位置，得到最大单位时间探测计数，根据探测效率计算公式计算得到被测探测器的探测效率峰值；

d） 探测效率计算公式如下：

$$\eta=\frac{N}{\mu}\ln\left(\frac{1-\frac{R_{dc}}{f_g}}{1-\frac{R_{de}}{f_g}}\right)$$

式中：

μ ——光脉冲的平均光子数；

η ——探测效率；
R_{dc} ——单位时间暗计数；
R_{de} ——单位时间探测计数；
f_p ——光源脉冲重复频率；
f_g ——探测器工作频率；
N ——$\frac{f_g}{f_p}$。

e) 重复上述步骤，并在测试中设置不同的光脉冲波长（波长范围应覆盖量子密钥分配产品的有效工作波长范围），依次测量得到每个通道单光子探测器在不同工作波长下的最大探测效率。

——通过标准：不同通道探测器在工作波长范围内的探测效率波长响应曲线对比度小于10%。

注：接收端使用多个单光子探测器时，应做单光子探测器波长相关性攻击防护的相关检测。

7.2.3.4 休眠时间攻击防护

——检测条件：厂商应提供相关设计文档以供审查。
——检测方法：通过审查送检文档，核实量子密钥分配产品是否具备对单光子探测器休眠时间攻击防护的相应设计。
——通过标准：量子密钥分配产品具备对探测器内APD的反向偏置电压进行实时检测，或保证所有探测器通道同时进入休眠时间并同时从休眠时间状态恢复的相应设计。

注：接收端使用基于APD的单光子探测器时，应做单光子探测器休眠时间攻击防护的相关检测。

7.2.3.5 门后攻击防护

——检测条件：厂商应提供相关设计文档以供审查。
——检测方法：通过审查送检文档，核实量子密钥分配产品是否具备对单光子探测器门后攻击防护的相应设计。
——通过标准：量子密钥分配产品具备对两个连续的探测响应的时间间隔进行监测并在低于安全阈值时进行告警，或在进入探测器前加一个监视器对计数异常进行告警，或分析光子探测时间是否处于有效探测窗口并丢弃处于探测窗口外计数的相应设计。

注：接收端使用基于APD的单光子探测器时，应做单光子探测器门后攻击防护的相关检测。

7.2.3.6 雪崩过渡区攻击防护

——检测条件：厂商应提供相关设计文档以供审查。
——检测方法：通过审查送检文档，核实量子密钥分配产品是否具备对单光子探测器雪崩过渡区攻击防护的相应设计。
——通过标准：QKD对光脉冲到达探测器的实际时间进行监测，当实际到达时间与预计时间差超过阈值，则QKD进行告警。

注：接收端使用基于APD的单光子探测器时，应做单光子探测器雪崩过渡区攻击防护的相关检测。

7.3 量子密钥分配产品检测

7.3.1 基本检测

7.3.1.1 功能检测

7.3.1.1.1 协议实现要求

检测方法：见7.1、7.2。

7.3.1.1.2 共享密钥随机性

——检测条件：待测量子密钥分配产品应具有采集共享密钥的检测接口。

——检测方法：

a) 按 5.2.2.2 中图 16 连接待测量子密钥分配产品，正常运行系统；

b) 通过检测接口采集并导出发送端和接收端生成的共享密钥，采集的密钥的样本量符合 GB/T 32915 的要求；

c) 按照 GB/T 32915 的要求对密钥的随机性进行检测。

——通过标准：检测结果应符合 GB/T 32915 的要求。

7.3.1.1.3 共享密钥一致性

——检测条件：待测量子密钥分配产品应具有采集共享密钥的检测接口。

——检测方法：

a) 按 5.2.2.2 中图 16 连接待测量子密钥分配产品，正常运行系统；

b) 通过检测接口采集并导出发送端和接收端生成的共享密钥；

c) 检测发送端和接收端生成的共享密钥的一致性。

——通过标准：发送端与接收端生成的共享密钥应一致。

7.3.1.2 性能检测

7.3.1.2.1 共享密钥生成率

——检测方法：

a) 按 5.2.2.2 中图 17 连接待测量子密钥分配产品，在发送端与接收端之间的量子信道连接可调衰减器或特定长度的光纤；

b) 在量子密钥分配产品正常运行状态后，统计量子密钥分配产品在此量子信道衰减环境下的共享密钥生成率。共享密钥生成率 $r=M/T$，其中 T 指单位时间、M 指单位时间内量子密钥分配产品产生的共享密钥总量。共享密钥生成率的单位可用 bps 的形式表示。

——通过标准：量子密钥分配产品的共享密钥生成率应符合产品送检文档中规定的共享密钥生成率的要求。

7.3.1.2.2 最大距离

——检测方法：

a) 按 5.2.2.2 中图 17 连接待测量子密钥分配产品，在发送端和接收端之间的量子信道连接可调衰减器或特定长度的光纤；

b) 通过增加量子信道的光纤盘长度或可调衰减器的衰减值，逐渐增加量子信道的衰减，直至量子密钥分配产品的共享密钥生成率小于用户使用需求的下限值，记录此时量子信道的距离（衰减）。

——通过标准：量子密钥分配产品最大距离应符合产品送检文档中规定的最大距离的要求。

7.3.1.2.3 环境适应性

——检测方法：根据 GB/T 2423.1 和 GB/T 2423.2 中规定的试验方法对量子密钥分配产品进行环境适应性试验。

——通过标准：量子密钥分配产品的环境适应性检测应达到 6.2.1.2.3 的要求，且环境适应性测试

过程中的产品运行相关评价参数应满足产品送检文档中规定的要求。

7.3.1.2.4 可靠性

——检测方法：根据 GB/T 5080.7 中规定的试验方法对量子密钥分配产品进行可靠性试验。

——通过标准：量子密钥分配产品的可靠性检测应符合 6.2.1.2.3 的要求，且可靠性测试过程中的产品运行相关评价参数应满足产品送检文档中规定的要求。

7.3.1.3 安全性设计检测

——检测方法：按照 GB/T 38625 中的检测规程和检测方法，对待测量子密钥分配产品的角色、服务和鉴别、物理安全、敏感安全参数管理及自测试等安全性设计进行检测。

7.3.2 鉴别检测

——检测条件：厂商应提供相关设计文档以供审查。

——检测方法：

a) 诱骗态 BB84 协议流程的对基和安全增强阶段的鉴别机制检测方法见 7.1.10、7.1.12；

b) 通过文档审查、代码审查的方式检测量子密钥分配产品的发送端与接收端之间是否进行实体鉴别，量子密钥分配产品与共享密钥管理层系统、管理平台、管理工具之间是否进行实体鉴别和消息鉴别；鉴别过程中是否具备随机数或时间戳或流水号等措施，以抵御重放攻击。

——通过标准：检测结果应符合 6.2.2 的要求。

7.3.3 接口检测

——检测条件：厂商应提供相关设计文档以供审查。

——检测方法：按照 GB/T 38625 中的检测规程和检测方法，检测待测量子密钥分配产品的对外接口。

——通过标准：检测结果应符合 6.2.3 的要求。

7.3.4 随机数发生器检测

——检测条件：待测量子密钥分配产品应具备随机数采集接口。

——检测方法：

a) 检查量子密钥分配产品配用的随机数发生器是否已通过商用密码产品检测认证；

b) 按 5.2.2.3 中图 18 连接待测量子密钥分配产品，正常运行系统；

c) 按 GM/T 0062 中 D 类产品的检测要求对待测量子密钥分配产品中的随机数发生器进行检测。

——通过标准：检测结果应符合 6.2.4 的要求。

7.3.5 日志管理检测

——检测方法：

a) 通过模拟相关操作实现下列相关行为或事件，查看量子密钥分配产品日志内容是否包括：

1) 操作行为，包括登录认证、系统配置、密钥管理等操作；

2) 安全事件，包括与管理平台连接、密钥产生、密钥更新、密钥销毁等事件；

3) 异常事件，包括认证失败、非法访问、完整性校验失败等异常事件。

b) 模拟授权和非授权的登录对日志进行导出操作。

——通过标准：检测结果应符合 6.2.5 的要求。

7.3.6 远程管理检测

——检测条件：

a) 厂商应提供相关设计文档以供审查；

b) 具备实现对量子密钥分配产品的远程监控管理的管理中心设备或软件。

——检测方法：

a) 按 5.2.2.4 中图 19 连接好待测设备和陪测设备，并完成量子密钥分配产品和管理中心之间的连通性配置，进行量子密钥分配产品的远程设备监控等管理操作；

b) 通过文档审查、代码审查的方式检测量子密钥分配产品和管理中心是否通过安全协议建立安全通道，实现管理信息的安全传递。

——通过标准：检测结果应符合 6.2.6 的要求。

8 合格判定

第 7 章所列的检测项中，其任意一项检测结果不合格，判定为产品不合格。

附 录 A
（资料性）
检测仪器

表 A.1 检测仪器

编号	仪器(工具)名称	主要用途	主要选型参数
1	光功率计	测试绝对光功率或通过一段光纤的光功率相对损耗	接收功率范围、精度
2	单光子探测器	对单个光子进行探测和计数	工作频率、暗计数率
3	光谱分析仪	用于中心波长、光谱特性测试	波长精度
4	示波器	用于脉冲波形的测量与统计	模拟带宽
5	光电转换器	将光信号转化为电信号	模拟带宽
6	窄脉冲光源	输出脉冲光	重复频率、脉冲宽度
7	连续波光源	输出连续光	中心波长、输出功率
8	信号源	输出多路同源同步控制信号	频率、延时步距、通道数
9	脉冲计数器	以数据统计方式对信号频率进行精密测量	最大计数率
10	偏振分析仪	全面分析光信号偏振属性	波长范围
11	可调衰减器	控制对输入光功率的衰减；调节量子信道衰减	衰减范围、衰减步距
12	光合束器	用于将两束光或多束光合成一束光	插入损耗
13	环形器	用于将进入其任一端口的入射波，按照确定的方向顺序传入下一个端口	插入损耗、隔离度、串扰
14	反射镜(法拉第反射镜、保偏反射镜)	用于搭建相位量子密钥分配产品的基(态)制备误差检测环境	插入损耗
15	网络交换机	用于搭建经典信道的网络环境	端口数量、网络带宽
16	集线器	用于对经典信道的交互信息进行抓取	端口数量
17	检测用 PC	用于运行操作系统及检测软件	操作系统、CPU、内存、硬盘

参 考 文 献

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, 1984: 175-179.

[2] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum crytograph systems by tailored bright illumination[J]. Nature Photon. 2010, 4(10): 686-689.

[3] Makarov V, Anisimov A, Skaar J. Effects of detector effciency mismatch on security of quantum cryptosystems[J]. Phys. Rev. A, 2006, 74(2): 022313.

[4] Qi B, Fung C H F, Lo H K, et al. Time-shift attack in practical quantum cryptosystems[J]. Quantum Inf. Comput, 2007, 7: 073-082.

[5] Qi B, Fung C, Zhao Y, et al. Quantum hacking: attacking practical quantum key distribution systems[C]. Proc. SPIE 6710, Quantum Communications and Quantum Imaging V, 67100I, 2007.

[6] Zhao Y, Fung C, Qi B, et al. Quantum hacking: Experimental demonstration of timeshift attack against practical quantum key distribution systems[J]. Phys. Rev. A, 2008, 78(4): 042333.