



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	I
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 符号和缩略语	3
4.1 符号	3
4.2 缩略语	3
5 检测环境	3
5.1 测试参考点	3
5.2 检测环境	4
6 检测内容	12
6.1 协议实现要求检测	12
6.2 量子密钥分配产品检测	16
7 检测方法	18
7.1 协议实现要求检测	18
7.2 防攻击检测	27
7.3 量子密钥分配产品检测	30
8 合格判定	33
附录 A (资料性) 检测仪器	34
参考文献	35

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。

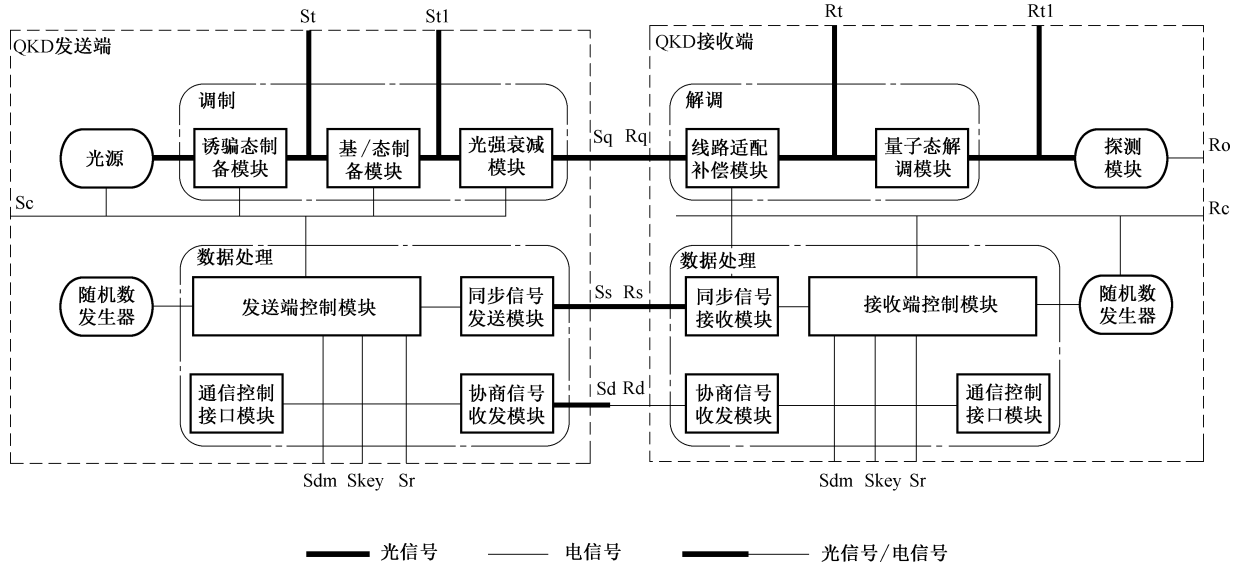


图 1 量子密钥分配产品配置和测试参考点

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。

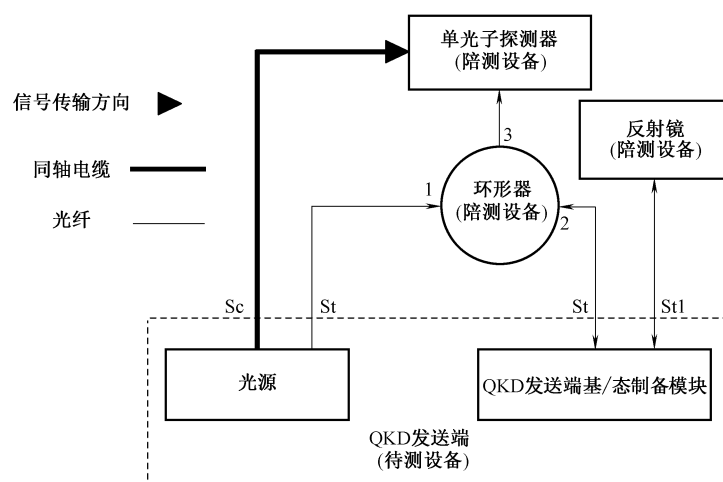


图2 编码基相对误差检测环境拓扑图(相位编码)

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。

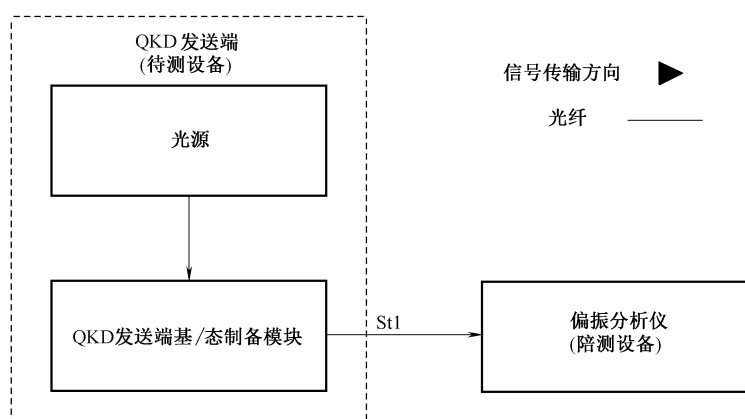


图3 编码基相对误差检测环境拓扑图(偏振编码)

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。

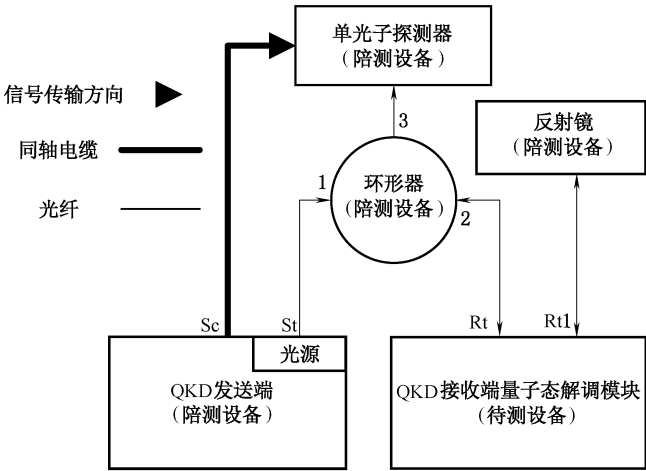


图 4 测量基相对误差检测环境拓扑图(相位编码)

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。

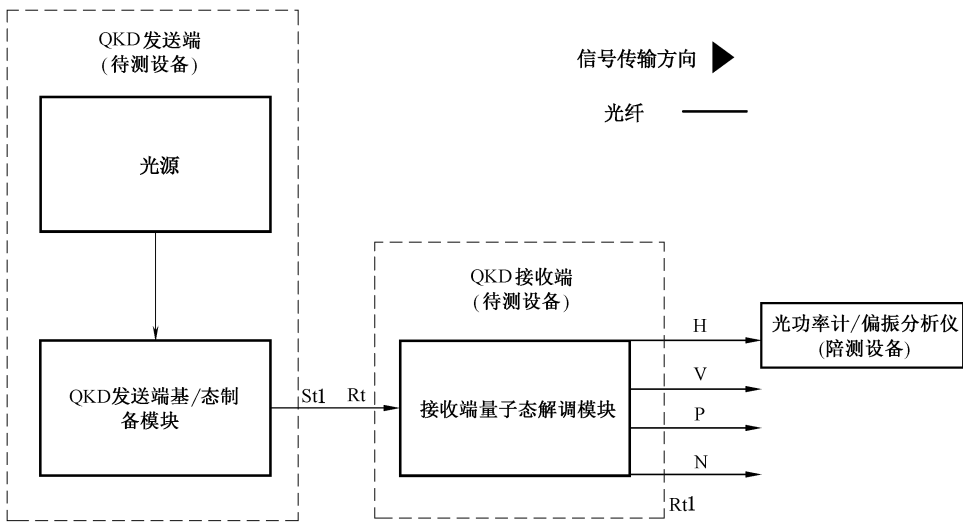


图 5 测量基相对误差检测环境拓扑图(偏振编码)

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。

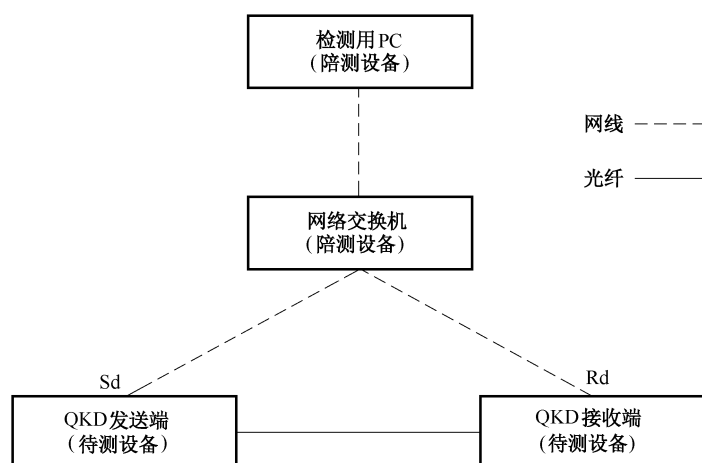


图6 编码基与测量基相对误差检测环境拓扑图

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。

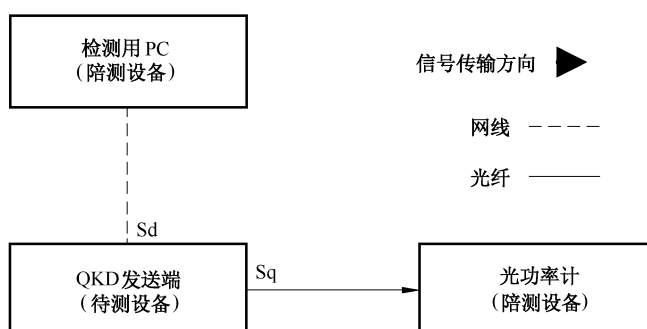


图7 光强制备检测环境拓扑图

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。

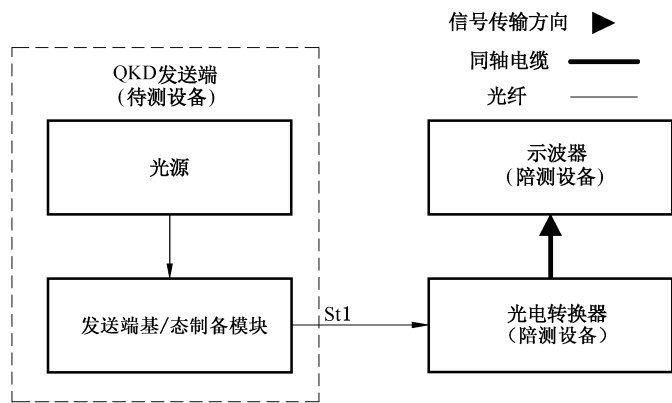


图 8 各种量子态幅度/脉宽检测环境拓扑图

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。

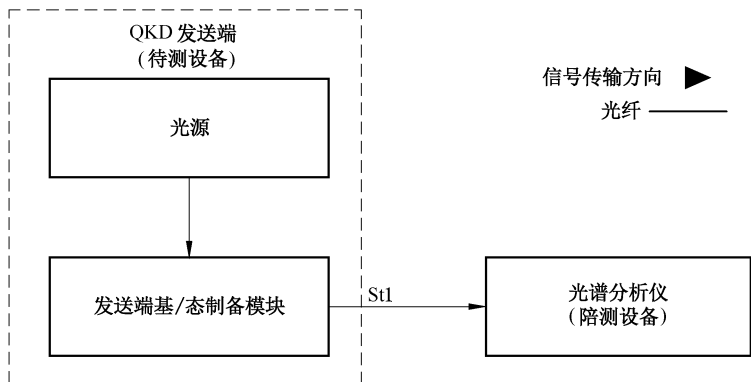


图 9 各种量子态光谱检测环境拓扑图

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。

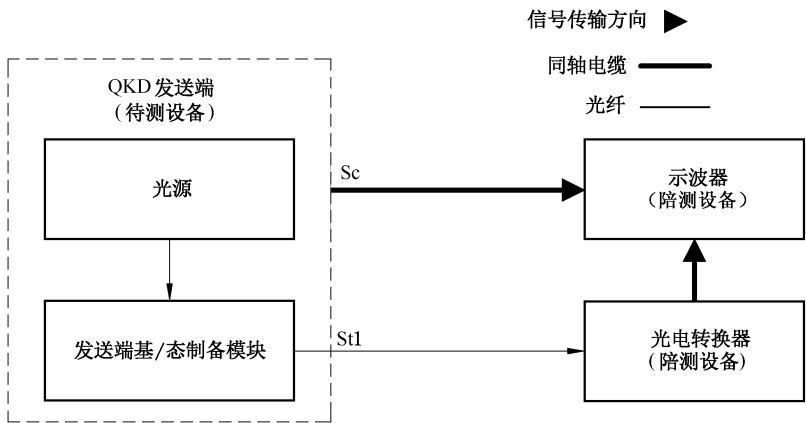


图 10 各种量子态时间检测环境拓扑图

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。

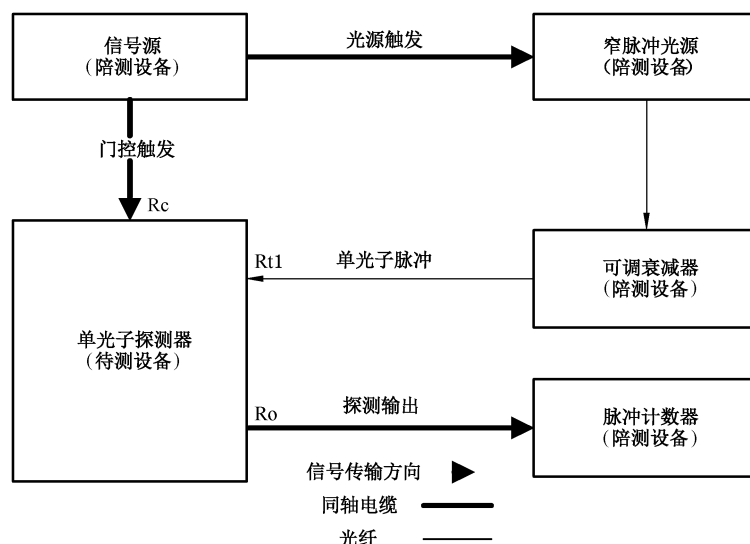


图 11 探测器关键属性检测环境拓扑图

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。

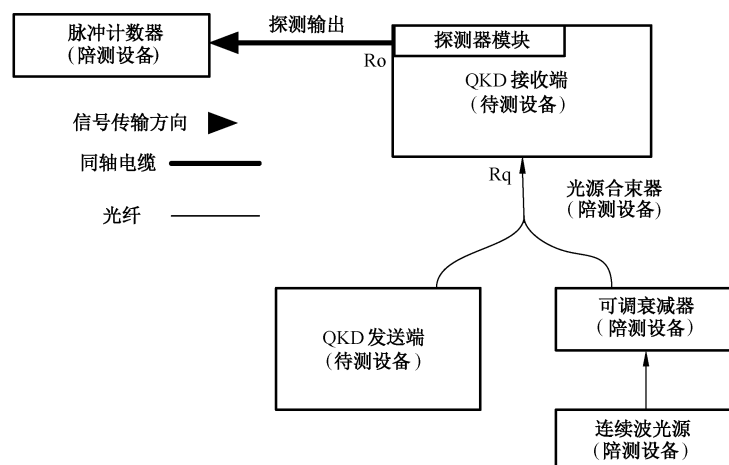


图 12 强光攻击防护检测环境拓扑图

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。

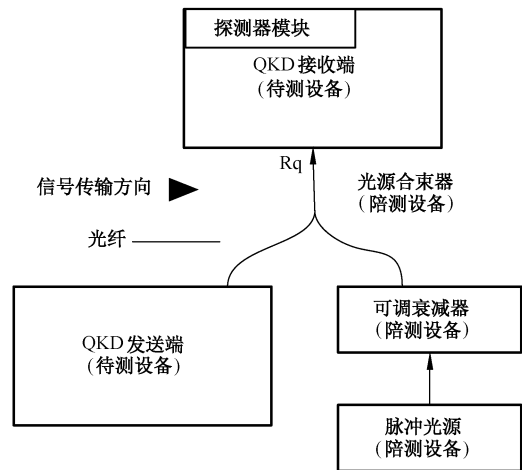


图 13 双计数攻击防护检测环境拓扑图

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。

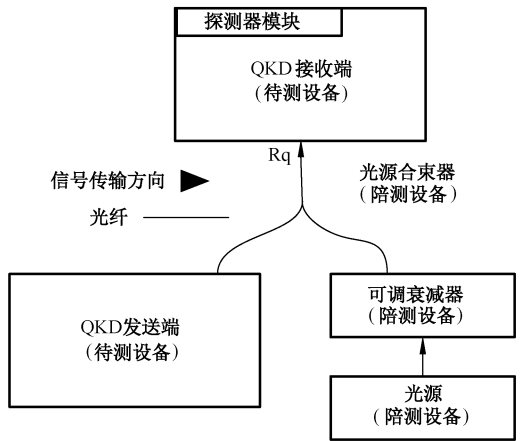


图 14 设备校准攻击防护检测环境拓扑图

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。

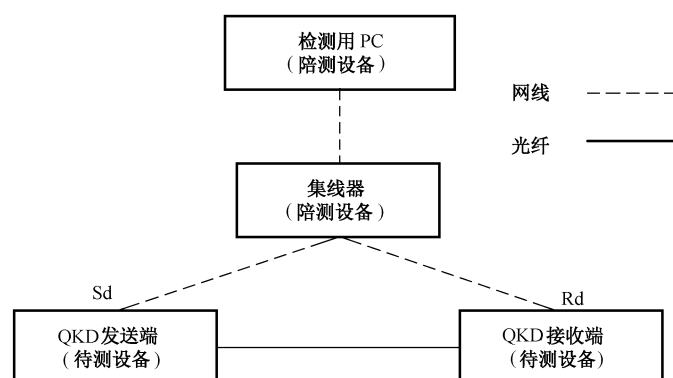


图 15 对基、纠错、安全增强过程检测环境拓扑图

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。

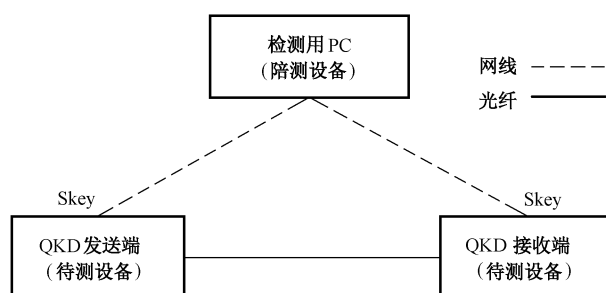


图 16 共享密钥随机性和一致性检测环境拓扑图

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。

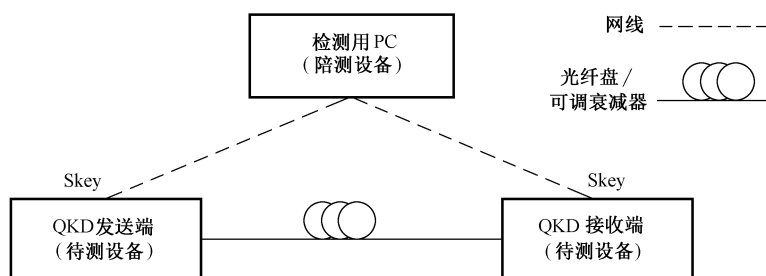


图 17 共享密钥生成率和最大距离检测环境拓扑图

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。

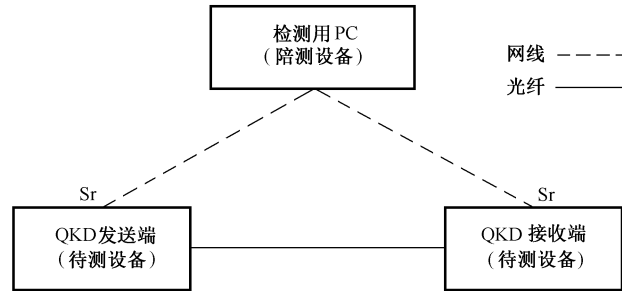


图 18 随机数发生器检测环境拓扑图

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。

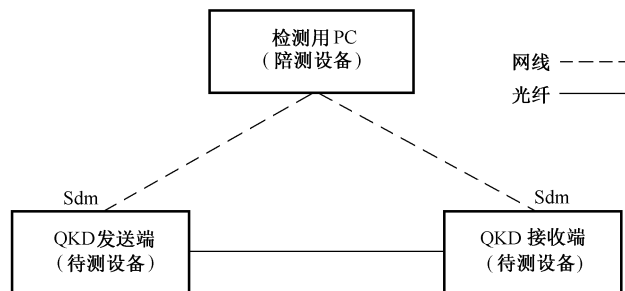


图 19 远程管理检测环境拓扑图

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 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 $\Phi^A = \{|\varphi_1^A\rangle, |\varphi_2^A\rangle\}$, $\Psi^A = \{|\Psi_1^A\rangle, |\Psi_2^A\rangle\}$, 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 $\epsilon_1 = \cos^{-1} |\langle \varphi_1^A | \varphi_1^B \rangle|$, $\epsilon_2 = \cos^{-1} |\langle \varphi_2^A | \varphi_2^B \rangle|$, $\epsilon_3 = \cos^{-1} |\langle \Psi_1^A | \Psi_1^B \rangle|$, $\epsilon_4 = \cos^{-1} |\langle \Psi_2^A | \Psi_2^B \rangle|$ 。编码基与测量基的相对误差定义为 $\frac{2}{\pi} \max(\epsilon_1, \epsilon_2, \epsilon_3, \epsilon_4)$ 。

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 $\epsilon = \frac{\pi}{2} - \theta$, 其中 $\theta = \arccos |\langle \varphi_1 | \varphi_2 \rangle|$; $|\Psi_1\rangle$ 与 $|\Psi_2\rangle$ 的正交误差

差定义为 $\epsilon' = \frac{\pi}{2} - \theta'$, 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:

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

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

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

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 $0 \leq \nu_2 < \nu_1 < \mu$;

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：

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

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：

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

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。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/927111060144006133>