



中华人民共和国密码行业标准

GM/T 0108—2021

诱骗态 BB84 量子密钥分配产品技术规范

Decoy-state BB84 quantum key distribution product technology 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

引言 II

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 4

5 概述 4

 5.1 量子密钥分配产品在量子保密通信系统的位置 4

 5.2 量子密钥分配产品的网络部署 5

6 诱骗态 BB84 协议实现要求 7

 6.1 概述及协议流程 7

 6.2 协议实现 8

7 量子密钥分配的产品要求 13

 7.1 基本要求 13

 7.2 鉴别要求 14

 7.3 接口要求 14

 7.4 随机数发生器 14

 7.5 日志管理 14

 7.6 远程管理 14

附录 A（资料性） 诱骗态 BB84 协议的简介 15

附录 B（资料性） 量子密钥分配产品的组成结构 16

附录 C（资料性） 抵御攻击与防护措施要求 17

附录 D（资料性） 纠错方法 18

附录 E（资料性） 安全增强方法 19

附录 F（资料性） 安全增强过程中压缩比的计算公式 21

参考文献 23

前 言

本文件按照 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、中国科学技术大学、中国人民解放军信息工程大学、科大国盾量子技术股份有限公司、中国电子科技集团第三十研究所、清华大学、北京大学、重庆大学、上海交通大学、北京邮电大学、南京邮电大学、哈尔滨工业大学、密码科学技术国家重点实验室、数据通信科学技术研究所、江苏亨通问天量子信息研究院有限公司、北京天融信网络安全技术有限公司、格尔软件股份有限公司。

本文件主要起草人：韩正甫、刘云、刘婧婧、苗春华、银振强、鲍皖苏、李宏伟、赵勇、徐兵杰、宋晨、凌杰、张启发、刘杰杰、王剑锋、龙桂鲁、郭弘、向宏、曾贵华、喻松、张一辰、王琴、李琼、韩琦、何远杭、黄伟、王宇、胡滨、苏琦、于宗文、李申、赵良圆、薛梦驰、李金国、赵梅生、唐世彪、彭翔、蔡斌、张春梅、黄鹏、郑强、费新伟。

引 言

量子密钥分配技术经历了多年的发展历程,已经得到广泛应用。其中,BB84 协议是由 Charles Henry Bennett 和 Gilles Brassard 在 1984 年提出的量子密钥分配协议,同时也是迄今为止最为成熟和应用最广的量子密钥分配协议,其理论安全性已得到严格的证明。为推动量子行业在我国信息安全领域的发展,本文件将涵盖采用弱相干态光源的诱骗态 BB84 协议及该类产品的要求规范。

诱骗态 BB84 量子密钥分配产品技术规范

1 范围

本文件基于采用弱相干态光源的诱骗态 BB84 协议,对协议各阶段的技术实现进行了规范,并对采用该协议的产品的的设计提出了基本要求。

本文件适用于诱骗态 BB84 协议的量子密钥分配产品的研制和检测。

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 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
- GM/T 0050 密码设备管理 设备管理技术规范
- GM/T 0062 密码产品随机数检测要求
- GM/Z 4001 密码术语

3 术语和定义

GB/T 37092、GM/T 0050 和 GM/Z 4001 界定的以及下列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

参数估计 parameter estimation

估算出量子比特误码率和相位误码率等参数的过程。

3.4

对基 basis sifting

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的相同基

矢的数据的过程,也称作筛选。

3.5

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。

3.6

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。

3.7

纠错后密钥 corrected key

筛后密钥经过纠错之后获得的数据。

3.8

经典信道 classical channel

传输除量子态以外的其他信息的信道。

3.9

量子保密通信系统 quantum secure communication system

利用量子密钥分配产品所产生的共享密钥实现安全通信的系统。

3.10

量子比特 qubit

量子信息的最小单位,物理上通常用一个二维量子态实现,数学上可用二维希尔伯特空间的一个单位向量来表示。

3.11

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。

3.12

量子比特误码率 quantum bit error rate

也称作误码率,是指筛后密钥的量子比特误码的比率,即筛后密钥中误码个数与筛后密钥长度的比值。

3.13

共享密钥 shared key

采用量子密钥分配协议所产生的对称密钥。

3.14

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。

3.15

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。

3.16

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。

3.17

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。

3.18

量子信道 quantum channel

传输量子态的信道。

3.19

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。

3.20

筛后密钥 sifted key

原始密钥经对基(筛选)之后获得的数据。

3.21

信号态 signal state

用以加载经典比特信息的量子态。

3.22

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。

3.23

相位误码率 phase error rate

一个量子比特发生相位翻转错误的比率,该数值被用于估计窃听者可能知晓的密钥信息的数量。

3.24

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。

3.25

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。诱骗态 BB84 协议的简介,见附录 A。

3.26

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。

3.27

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。

E_{μ} 实际的信号态的量子比特误码率

E_{v_1} 实际的诱骗态 1 的量子比特误码率

E_{v_2} 实际的诱骗态 2 的量子比特误码率

I_{ec} 纠错过程中暴露的信息量 $leak_{ec}$ 和被纠错后的密钥量 L_{CK} 的比值

$leak_{EC}$	纠错过程中暴露的信息量
L_{CK}	被纠错后的密钥量
M_{μ}	对基过程后接收端生成的信号态的筛后密钥的数量
M_{v_1}	对基过程后接收端生成的诱骗态 1 的筛后密钥的数量
M_{v_2}	对基过程后接收端生成的诱骗态 2 的筛后密钥的数量
N_{μ}	发送端发送信号态光脉冲的数量
N_{v_1}	发送端发送诱骗态 1 光脉冲的数量
N_{v_2}	发送端发送诱骗态 2 光脉冲的数量
Q_{μ}	接收端信号态的筛后密钥数量与发送端发送的信号态光脉冲数量的比值
Q_{v_1}	接收端诱骗态 1 的筛后密钥数量与发送端发送信号态光脉冲数量的比值
Q_{v_2}	接收端诱骗态 2 的筛后密钥数量与发送端发送信号态光脉冲数量的比值
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)

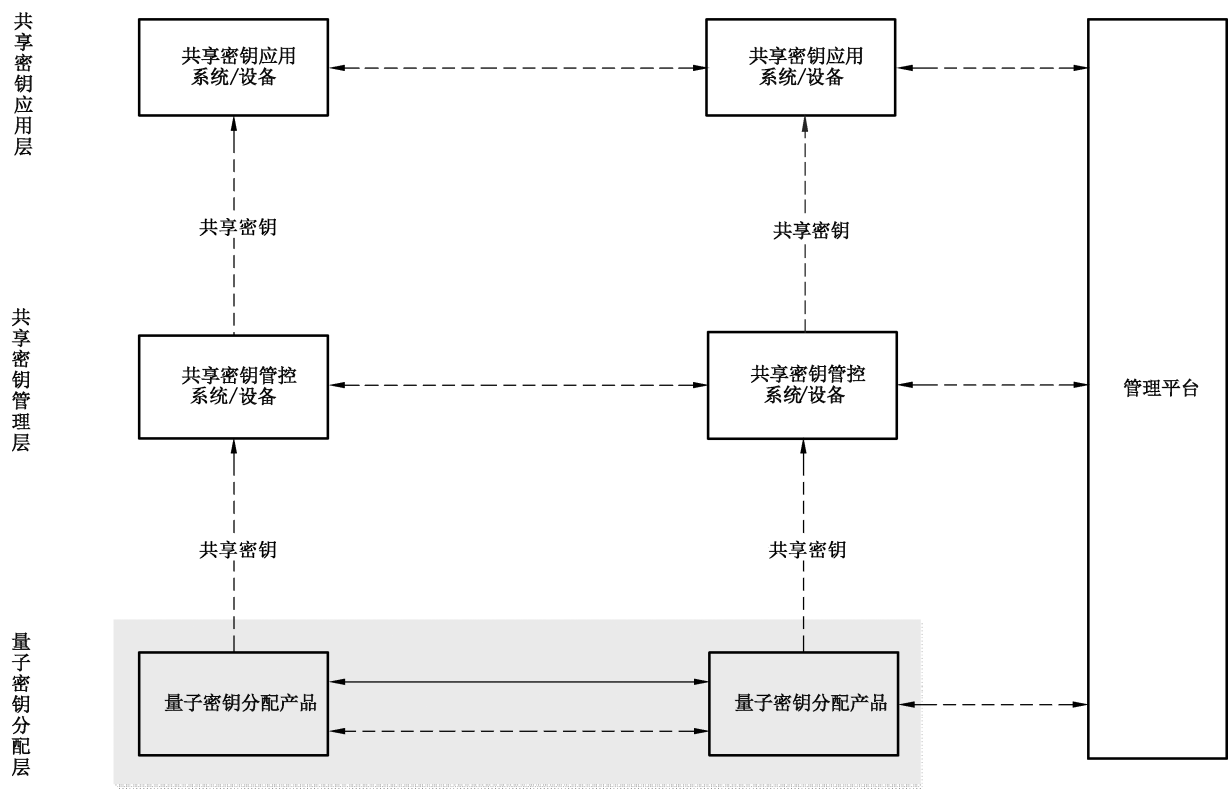
LDPC:低密度奇偶校验(Low Density Parity Check)

QKD:量子密钥分配(Quantum Key Distribution)

5 概述

5.1 量子密钥分配产品在量子保密通信系统的位置

量子密钥分配产品在量子保密通信系统的位置见图 1。



注：
--- 经典信道
— 量子信道

图 1 量子密钥分配产品在量子保密通信系统的位置

量子密钥分配层：主要包括量子密钥分配产品等，借助经典信道和量子信道，完成共享密钥的协商和分配，可为共享密钥管理层提供共享密钥。量子密钥分配产品的组成结构，见附录 B。

共享密钥管理层：可在经典信道中实现共享密钥的存储、传输和中继，为共享密钥应用层系统提供共享密钥的服务。

共享密钥应用层：主要包括共享密钥应用系统和设备，可通过经典信道，使用共享密钥管理层提供的共享密钥，实现传输数据加解密。

管理平台：主要包括量子网络管控系统，管控对象包括量子保密通信网络内的被管设备。通过经典信道实现对量子保密通信网络的监控和管理。

量子密钥分配层、共享密钥管理层、共享密钥应用层和管理平台组成量子保密通信系统。

本文件仅对量子密钥分配产品的技术实现进行规范。

5.2 量子密钥分配产品的网络部署

量子密钥分配产品的网络部署见图 2。要求量子密钥分配产品间应同时建立经典信道和量子信道，在量子信道中不应存在信号放大和再生的器件。

量子密钥分配产品间的经典信道可由局域网或广域网组成，量子信道可由光纤和无源光器件组成。通过网络部署，可实现量子密钥分配产品间一对一、一对多、多对一、多对多的应用场景。

经典信道网络安全不属于本标准规定的范围，但应采取网络安全的措施以保障经典信道的网络安全。

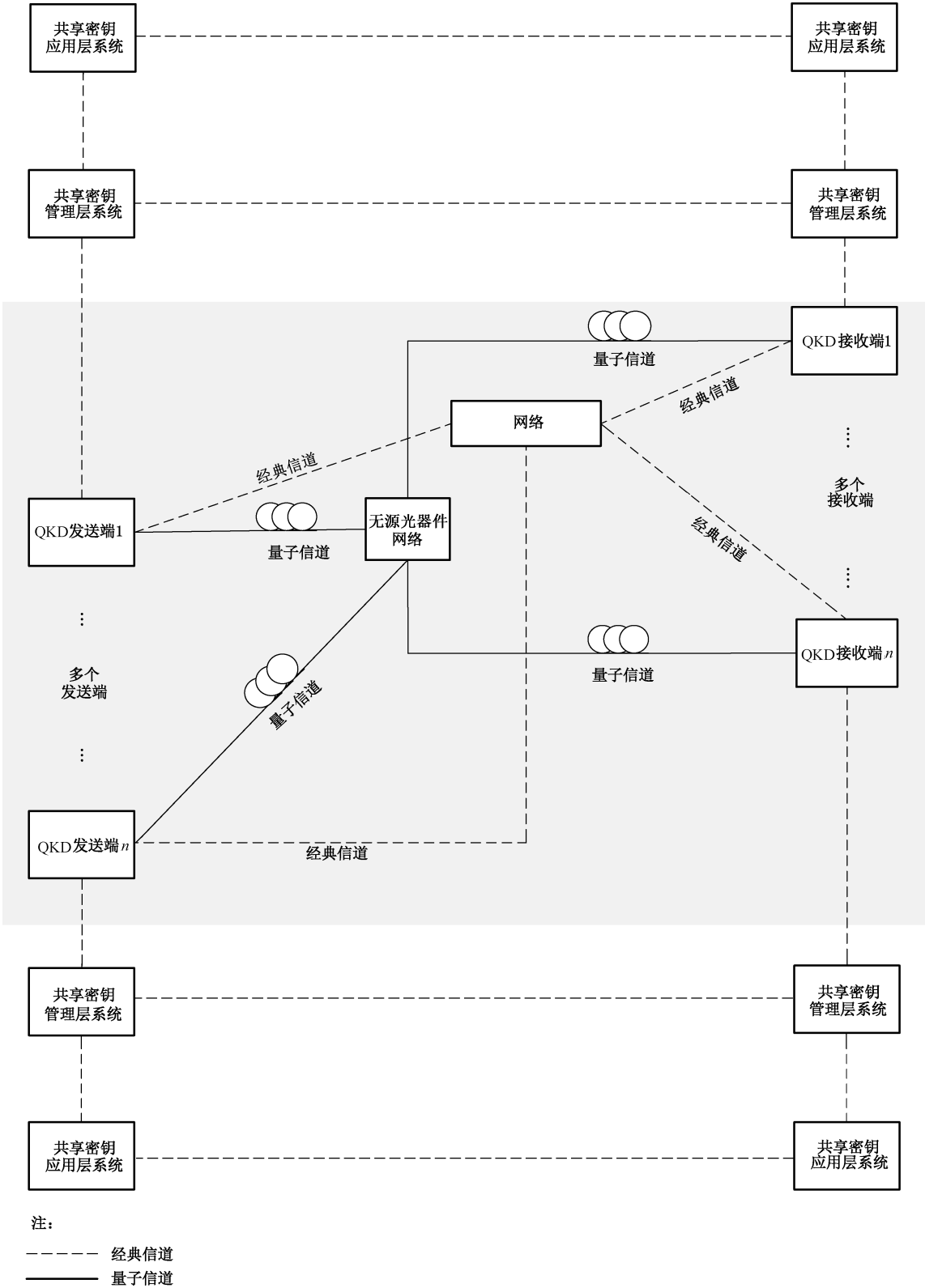


图 2 网络部署图

6 诱骗态 BB84 协议实现要求

6.1 概述及协议流程

6.1.1 概述

诱骗态 BB84 协议包括量子态制备、量子态传输、量子态测量、对基、纠错、安全增强等步骤，其协议简介，见附录 A。

6.1.2 协议基本流程

诱骗态 BB84 协议基本流程见图 3。

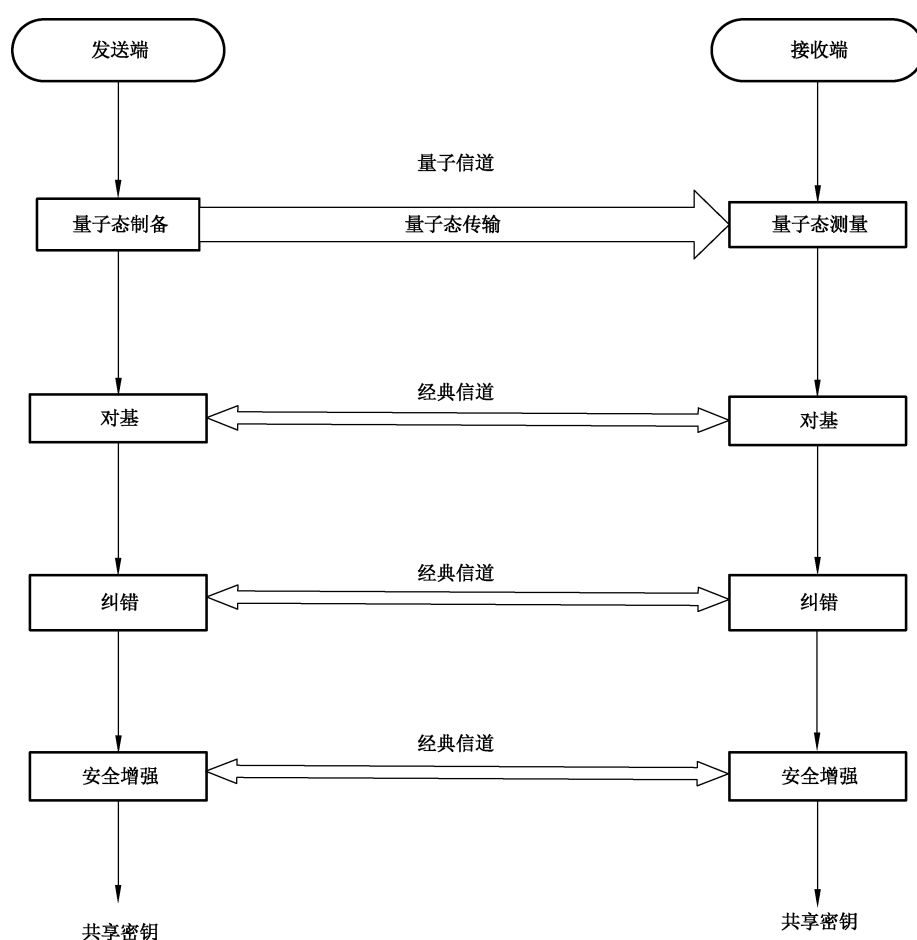


图 3 诱骗态 BB84 协议基本流程示意图

诱骗态 BB84 协议基本流程描述如下：

- 量子态制备：发送端制备量子态作为信息的载体，将用以加载信息的量子态随机加载在对应的光脉冲上，量子态可由偏振、相位、时间、自旋、动量等物理量表征。
- 量子态传输：发送端将加载了信息的量子态发送给接收端。
- 量子态测量：接收端随机选择测量基对发送端发来的已加载了信息的量子态进行测量，生成原始密钥。
- 对基：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探测所采用的测量基进行比

对,双方只保留使用相同基矢的数据,生成筛后密钥。

e) 纠错:发送端和接收端纠正两端筛后密钥中的量子比特误码,生成纠错后密钥。

f) 安全增强:发送端和接收端通过计算压缩比对纠错后密钥进行压缩,生成共享密钥。

6.2 协议实现

6.2.1 量子态制备

6.2.1.1 基和态的描述

态的描述:定义二维希尔伯特空间的四种量子态分别记为 $|\phi_1\rangle$ 、 $|\phi_2\rangle$ 、 $|\psi_1\rangle$ 、 $|\psi_2\rangle$ 。

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 $\Phi = \{|\phi_1\rangle, |\phi_2\rangle\}$, $\Psi = \{|\psi_1\rangle, |\psi_2\rangle\}$ 。

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 $|\phi_1\rangle$ 与经典比特“0”对应,量子态 $|\phi_2\rangle$ 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。

6.2.1.2 基和态的选择

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。

6.2.1.3 基制备要求

两组基共轭,即 Φ 和 Ψ 共轭。

定义 1:记 $A = |\langle\phi_1|\phi_1\rangle|$, $B = |\langle\phi_1|\phi_2\rangle|$, $C = |\langle\phi_2|\phi_1\rangle|$, $D = |\langle\phi_2|\phi_2\rangle|$,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 $\Phi^A = \{|\phi_1^A\rangle, |\phi_2^A\rangle\}$, $\Psi^A = \{|\psi_1^A\rangle, |\psi_2^A\rangle\}$,接收端与之对应的两组基分别记为 Φ^B 与 Ψ^B ,其中 $\Phi^B = \{|\phi_1^B\rangle, |\phi_2^B\rangle\}$, $\Psi^B = \{|\psi_1^B\rangle, |\psi_2^B\rangle\}$ 。记 $\epsilon_1 = \cos^{-1}|\langle\phi_1^A|\phi_1^B\rangle|$, $\epsilon_2 = \cos^{-1}|\langle\phi_2^A|\phi_2^B\rangle|$, $\epsilon_3 = \cos^{-1}|\langle\psi_1^A|\psi_1^B\rangle|$, $\epsilon_4 = \cos^{-1}|\langle\psi_2^A|\psi_2^B\rangle|$ 。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%。

6.2.1.4 态制备要求

每组基的两种量子态应正交,即 $|\phi_1\rangle$ 与 $|\phi_2\rangle$ 正交, $|\psi_1\rangle$ 与 $|\psi_2\rangle$ 正交。

定义: $|\phi_1\rangle$ 与 $|\phi_2\rangle$ 的正交误差定义为 $\epsilon = \frac{\pi}{2} - \theta$,其中 $\theta = \arccos|\langle\phi_1|\phi_2\rangle|$; $|\psi_1\rangle$ 与 $|\psi_2\rangle$ 的正交误差

定义为 $\epsilon' = \frac{\pi}{2} - \theta'$,其中 $\theta' = \arccos|\langle\psi_1|\psi_2\rangle|$ 。

要求:

- a) $|\phi_1\rangle$ 与 $|\phi_2\rangle$ 的正交误差应满足：

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

- b) $|\psi_1\rangle$ 与 $|\psi_2\rangle$ 的正交误差应满足：

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

6.2.1.5 光强制备要求

发送端制备量子态作为量子信息的载体。量子态是通过光源发射的、具有不同强度的光脉冲。

以诱骗态协议中常使用的三态协议为例,量子态具有三种不同强度,可分别作为信号态、诱骗态 1、诱骗态 2。

定义:信号态是平均光子数为 μ 的光脉冲;诱骗态 1 光脉冲是平均光子数为 ν_1 的光脉冲;诱骗态 2 光脉冲是平均光子数为 ν_2 的光脉冲。

要求：

- a) 信号态、诱骗态 1、诱骗态 2 光脉冲的强度应满足 $0 \leq \nu_2 < \nu_1 < \mu, \nu_2 + \nu_1 < \mu$;
b) 同种强度的量子态应满足：

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

式中：

p' ——实际光脉冲强度；

p ——理论光脉冲强度。

6.2.1.6 其他属性制备要求

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：

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

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。

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/677102200144006133>