ICS 35.030
CCS L 80

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

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了相同基

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。

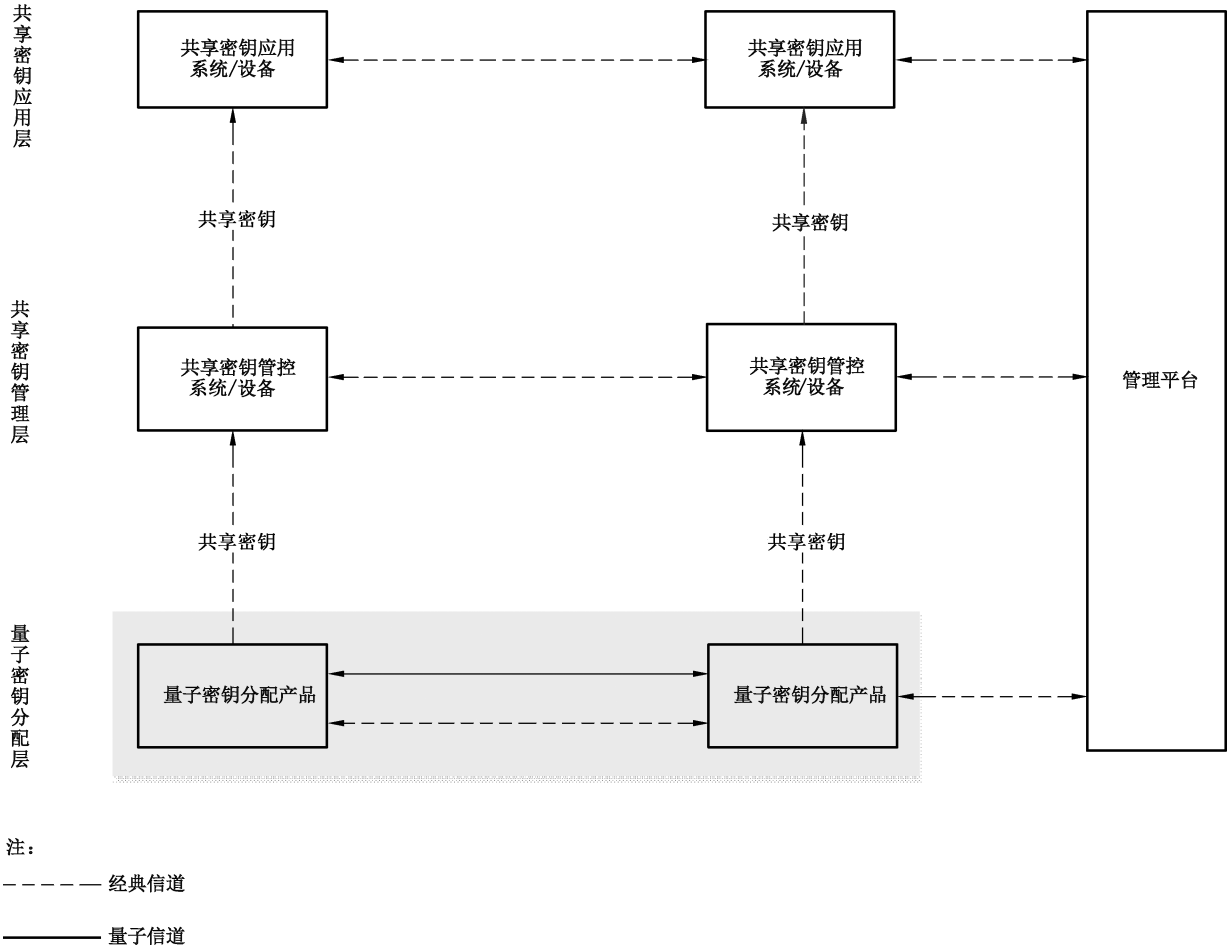

图 1　量子密钥分配产品在量子保密通信系统的位置

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。

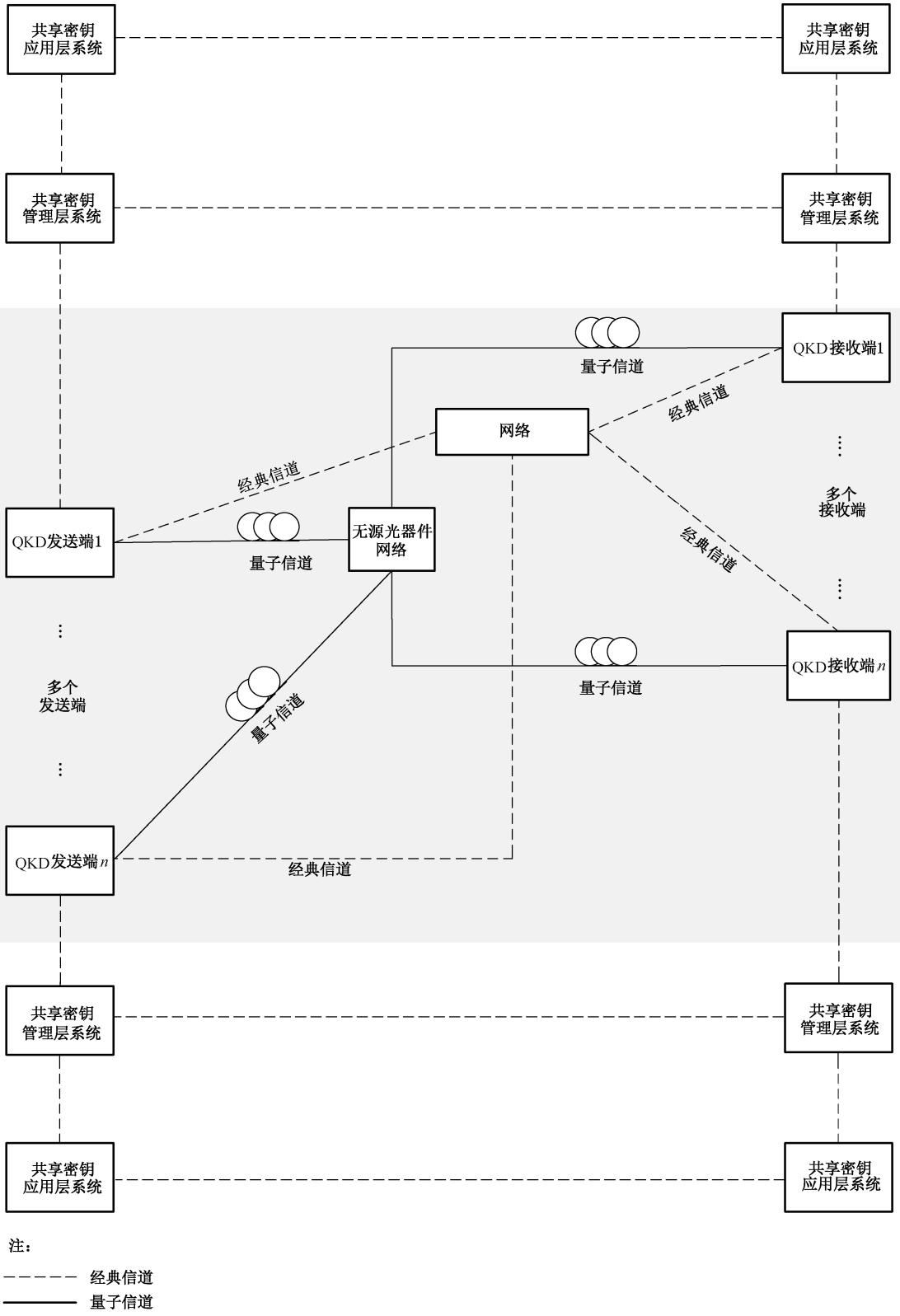
共享密钥
应用层系统
共享密钥
应用层系统
共享密钥
管理层系统
共享密钥
管理层系统
量子信道
QKD接收端1
经典信道
网络
经典信道
多个
接收端
QKD发送端1
量子信道
无源光器件
网络
经典信道
多个
发送端
量子信道
QKD接收端n
量子信道
QKD发送端n
经典信道
共享密钥
管理层系统
共享密钥
管理层系统
共享密钥
应用层系统
共享密钥
应用层系统
注：
经典信道
量子信道

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。

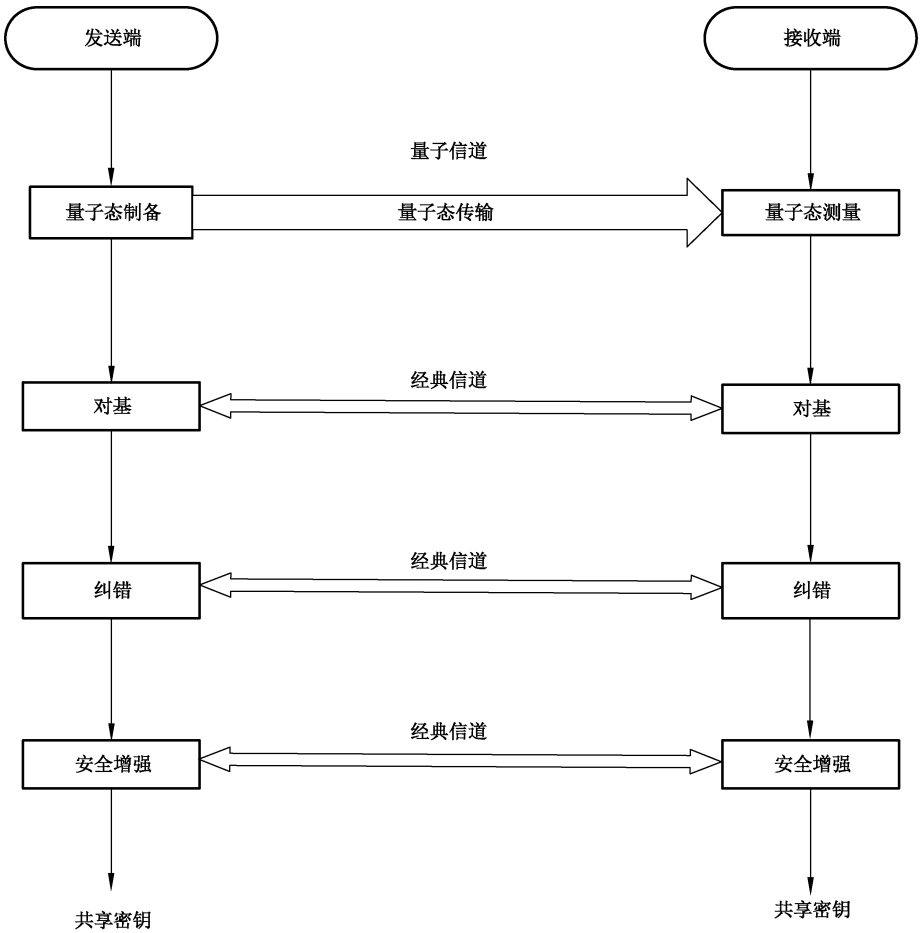

图 3 诱骗态 BB84 协议基本流程示意图

诱骗态 BB84 协议基本流程描述如下：

a) 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。

b) 量子态传输：发送端将加载了信息的量子态发送给接收端。

c) 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。

d) 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$|\phi_1\rangle$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 $A=|\langle\phi_1|\psi_1\rangle|$，$B=|\langle\phi_1|\psi_2\rangle|$，$C=|\langle\phi_2|\psi_1\rangle|$，$D=|\langle\phi_2|\psi_2\rangle|$，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 $\Phi^A=\{|\phi_1^A\rangle,|\phi_2^A\rangle\}$，$\Psi=\{|\psi_1^A\rangle,|\psi_2^A\rangle\}$，接收端与之对应的两组基分别记为 Φ^B 与 Ψ^B，其中 $\Phi^B=\{|\phi_1^B\rangle,|\phi_2^B\rangle\}$，$\Psi^B=\{|\psi_1^B\rangle,|\psi_2^B\rangle\}$。记 $\varepsilon_1=\cos^{-1}|\langle\phi_1^A|\phi_1^B\rangle|$，$\varepsilon_2=\cos^{-1}|\langle\phi_2^A|\phi_2^B\rangle|$，$\varepsilon_3=\cos^{-1}|\langle\psi_1^A|\psi_1^B\rangle|$，$\varepsilon_4=\cos^{-1}|\langle\psi_2^A|\psi_2^B\rangle|$。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%。

6.2.1.4 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 $\varepsilon=\frac{\pi}{2}-\theta$，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 $\varepsilon'=\frac{\pi}{2}-\theta'$，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：

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

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

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

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$0\leqslant\nu_2<\nu_1<\mu$、$\nu_2+\nu_1<\mu$；

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。

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：

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

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[0,2π)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。

6.2.1.7 编码

编码过程，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。

编码即信息加载的过程，编码过程应符合如下要求：

a) 依据随机数发生器输出的物理随机序列，通过6.2.1.1中约定的二进制比特0、1与基和量子态的对应关系，确定需要编码的量子态；

b) 根据a)中确定的量子态信息，将用以加载信息的量子态调制到对应的光脉冲上，并保存加载在量子态上的经典比特信息。

其中，执行b)时，需按照信号态、诱骗态1、诱骗态2的光脉冲发送数量的预设比例要求，随机制备6.2.1.5和6.2.1.6中规定要求的特定强度的光脉冲；需按照两组基的制备数量的预设比例要求，随机制备的编码基和量子态光应遵循本标准6.2.1.3和6.2.1.4的要求。

在编码过程中，应至少具有抵御特洛伊攻击、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，见附录C中a)。

6.2.2 量子态传输

发送端按照本标准6.2.1的要求，将加载了信息的量子态通过量子信道发送给接收端，并记录所发光脉冲的光强制备信息和编码信息。

6.2.3 量子态测量

6.2.3.1 解码

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。

解码过程应符合如下要求：

依据随机数发生器输出的物理随机序列，通过6.2.1.1中约定的二进制比特0、1与基的对应关系，选择需要测量量子态所用的测量基，对量子态进行解调。测量基的制备应遵循6.2.1.3的要求；两组基制备数量的比例应按照产品预设要求。

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，见附录C中b)、c)、d)、e)、f)。

6.2.3.2 探测

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。

探测过程应符合如下基本要求、接口要求和关键属性要求：

a) 基本要求：

量子密钥分配产品在探测过程中，若接收端通过多个探测器时，应至少具有抵御双计数攻击的能力。

量子密钥分配产品在探测过程中，若接收端通过基于 APD 的单光子探测器，应至少具有抵御强光攻击、死时间攻击、门后攻击和雪崩过渡区攻击的能力。

抵御探测过程中的相关攻击可采用的推荐措施，见附录 C 中 g)、h)、i)、j)、k)。

b) 接口要求：

1) 单光子探测器接口应包括量子信号接口、光电转换后的电脉冲输出接口、电源接口；

2) 如果单光子探测器集成在量子密钥分配产品内部时，可与其他模块有相连接的内部接口（例如串口、网口、I2C、自定义总线等），用于单光子探测器的运行状态上报（例如温度、电压、探测计数统计等上报，异常、攻击检测等上报）、特定运行流程控制命令下发（仅接收特定几种运行流程控制命令，如启动门控探测器的延时扫描、多个单光子探测器的效率均衡自校准（采用内部光源））。

c) 关键属性要求：

门控模式单光子探测器，应满足如下 a)、b)的要求；自由运行模式探测器，应满足如下 b)要求；当接收端采用主动基矢选择方案进行量子态解码，且每个探测器的探测结果随机表示 0 或 1 的信息时，可不满足如下 a)、b)的要求。

1) 多通道探测器通道间探测效率半高宽应满足：

$$\frac{w_{max}-w_{min}}{w_{avg}}<10\%$$

式中：

w_{max}——最大半高宽；

w_{min}——最小半高宽；

w_{avg}——所有通道探测效率半高宽平均值。

2) 多通道探测器通道间探测效率峰值应满足：

$$\frac{\eta_{max}-\eta_{min}}{\eta_{avg}}<10\%$$

式中：

η_{max}——最大探测效率；

η_{min}——最小探测效率；

η_{avg}——所有通道的探测效率平均值。

6.2.4 对基

6.2.4.1 对基

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。

对基过程应符合如下逻辑要求和通信要求：

a) 逻辑要求：

1） 接收端通过经典信道将探测到的每个量子态所用的测量基与位置信息告知发送端；
2） 发送端将接收端探测到的每个量子态所用的测量基与制备这些量子态时所用的编码基进行比较；
3） 发送端通过经典信道将上述基比对结果告知接收端，但不得透露其他信息；
4） 若基比对结果为一致，则双方保留原始密钥，生成筛后密钥；若基比对结果为不一致，则双方应丢弃原始密钥。

b） 通信要求：
1） 接收端通过经典信道向发送端传送的可公开信息包括测量基信息、测量到的光脉冲位置信息；
2） 发送端通过经典信道向接收端传送的可公开信息包括发送的光脉冲位置信息、光脉冲强度信息、基比对结果；
3） 对基过程中交互的全部信息应执行鉴别过程，过程应遵循 GB/T 15852.1 或GB/T 15852.2 或 GB/T 15852.3，其实现过程中所需的密钥应事先预置。

6.2.4.2 参数估计

对基过程应同时对 Q_{μ} 和 Q_{v1} 进行统计，结果用于安全增强阶段的压缩比计算。

6.2.5 纠错

6.2.5.1 参数估计

纠错方法执行前，发送端和接收端通过分析筛后密钥，估算量子比特误码率，用于优化算法，提高效率，并根据判别条件确认是否终止协议流程。

参数估计的过程应符合如下要求：

a） 对筛后密钥量子比特误码率的估算。

b） 量子比特误码率的估算值 E'_{μ} 可用于设置和调整纠错方法的运行参数。估算的方法包括：根据运行环境和其他性能参数估算出的量子比特误码率；或者通过随机采样实时估算筛后密钥的量子比特误码率；或者通过上一次筛后密钥的实际量子比特误码率估算筛后密钥的量子比特误码率。

c） 在理想情况下，BB84 协议的安全密钥生成率不超过 $1-2H(\sigma)$，其中 H 是二元香农熵，当误码率 $\sigma=11\%$ 时，安全密钥生成率为 0。若 $E'_{\mu}\geqslant\rho$，$\rho\in[0,11\%]$，则判定系统不安全，终止剩余的步骤；若 $E'_{\mu}<\rho$，$\rho\in[0,11\%]$，则判定系统安全，继续执行。

注：当纠错方法不需要量子比特误码率作为运行参数时，可不执行 6.2.5.1 的参数估计；c）中系统安全的判定，可在此处不执行，而在 6.2.5.2 步骤 e）中使用 E_{μ} 执行。

6.2.5.2 纠错

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。

纠错过程应符合如下要求：

a） 为了纠正发送端和接收端双方筛后密钥中的量子比特误码，采用纠错方法对筛后密钥进行纠错，推荐的纠错方法参见附录 D。

b） 为了判断发送端和接收端的密钥是否相同，假设密钥分别为 K_A 和 K_B，应采用数据校验的方法，判定 K_A 和 K_B 是否相同。

c） 若 $K_A=K_B$，则判定纠错成功，该组密钥保留，继续执行下一阶段的步骤；若 $K_A\neq K_B$，则判定

纠错不成功，终止剩余的步骤。

d) 记录实际被纠正的由信号态、诱骗态 1 和诱骗态 2 生成的筛后密钥的错误比特的数量，即实际量子比特误码的数量 ME_{μ}、ME_{ν_1}、ME_{ν_2}。

e) 计算实际的信号态、诱骗态 1 和诱骗态 2 的量子比特误码率 $E_{\mu}=\frac{ME_{\mu}}{M_{\mu}}$，$E_{\nu_1}=\frac{ME_{\nu_1}}{M_{\nu_1}}$，$E_{\nu_2}=\frac{ME_{\nu_2}}{M_{\nu_2}}$。

f) 记录所有纠错过程中暴露的信息量 $leak_{EC}$，用于安全增强阶段使用。

注：如果诱骗态量子比特误码率通过发送端和接收端双方公开信息而获得，则不需要对诱骗态执行 d)～e)过程。

6.2.6 安全增强

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。推荐的杂凑函数类，见附录 E。

安全增强过程应符合如下要求：

a) 安全增强过程的输入为纠错后密钥，输出为共享密钥。

b) 结合对基过程和纠错过程估算或统计的参数，估算出安全增强过程中的压缩比 R，即“共享密钥量/纠错后密钥量”，压缩比 R 根据 6.2.5.1 计算，压缩比 R 的计算公式见附录 F。

c) 安全增强过程中交互的全部信息，都应执行鉴别过程，进行消息源合法性和数据完整性的检验，鉴别过程可遵循 GB/T 15852.1 或 GB/T 15852.2 或 GB/T 15852.3，其实现过程中所需的密钥应事先预置。

7 量子密钥分配的产品要求

7.1 基本要求

7.1.1 功能要求

量子密钥分配产品应遵循诱骗态 BB84 协议，遵循 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遵循 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。

7.1.2 性能要求

7.1.2.1 共享密钥生成率

定义：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 b/s 的形式表示。

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。

7.1.2.2 最大距离

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。

7.1.2.3 环境适应性和可靠性

量子密钥分配产品的工作环境应根据实际应遵循 GB/T 2423.1 和 GB/T 2423.2 的要求。

量子密钥分配产品的平均无故障工作时间应不低于 4 000 h。

7.1.3 安全性设计要求

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安全性设计应遵循 GB/T 37092 的要求。

7.2 鉴别要求

本文件中诱骗态 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，鉴别机制应遵循 GB/T 15852.1 或 GB/T 15852.2 或 GB/T 15852.3 的要求。

本文件中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，鉴别机制应遵循 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，鉴别机制应遵循 GB/T 15843.2 或 GB/T 15843.4 的要求。它们之间交互的全部信息也应采用消息鉴别，鉴别机制应遵循 GB/T 15852.1 或 GB/T 15852.2 或 GB/T 15852.3 的要求。

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。

在鉴别过程中，应至少具有抵御重放攻击的能力。

抵御鉴别过程中的相关攻击可采用的推荐措施，见附录 C 中 l)。

7.3 接口要求

量子密钥分配产品应至少具备量子信道接口、经典信道接口和共享密钥应用接口。量子信道接口用于量子态的输入和输出；经典信道接口用于数据、控制信息的输入，以及数据、控制信息和状态信息的输出；共享密钥应用接口为应用服务提供共享密钥输出。

量子信道接口应为光纤接口，经典信道接口和共享密钥应用接口可采用以太网、串口、USB 或者其他接口形式与外部设备连接。

7.4 随机数发生器

量子密钥分配产品配用的随机数发生器应通过商用密码产品检测认证。

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，应遵循 GM/T 0062 中 D 类产品的要求。

7.5 日志管理

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。

7.6 远程管理

量子密钥分配产品可具有远程管理功能，用于远程密钥管理、远程设备监控、远程设备参数配置等。

量子密钥分配产品远程管理功能的实现应遵循 GM/T 0050 的要求。

附 录 A
（资料性）
诱骗态 BB84 协议的简介

BB84 协议是历史上第一个量子密钥分配协议，由 Charles Henry Bennett 与 Gilles Brassard 于 1984 年提出。在所有的量子密钥分配协议研究中，关于 BB84 协议的研究最为丰富和深入，包括最早的 Mayers，Lo-Chau，Shor-Preskill 等基于理想模型的安全性分析，后来的 GLLP、诱骗态等基于实际系统模型的安全性分析，以及有限码长、偏置基矢选择、相位随机化、光强涨落等问题的研究。在密码学领域中，被研究的深入程度和时间长短是衡量一个密码协议安全性能的重要指标。从这个层面上来说，BB84 协议无疑是一种具备高强度安全性的量子密钥分配协议。

原始的 BB84 协议要求发送端使用理想单光子源进行量子态的制备。然而，后者技术尚不成熟，实验者只能借助技术成熟、成本较低的半导体激光器制备弱相干态光来近似模拟理想单光子源。然而，弱相干态光以一定的概率含有多光子成分，使得 BB84 协议受光子数分束攻击的威胁，因此其安全成码率会受到很大限制。在这样的背景下，诱骗态技术应运而生。该技术通过在激光器发射的信号光中随机掺杂一些不同强度的诱骗光来监测信道和窃听者对光脉冲的影响。结合诱骗态技术，即便使用弱相干态光源，BB84 协议的成码率也几乎与使用理想单光子源的协议一样。因此，在实验室和工程化实践中，诱骗态 BB84 协议受到广泛采纳。

附 录 B
（资料性）
量子密钥分配产品的组成结构

量子密钥分配产品由发送端和接收端构成，两者通过量子信道和经典信道连接，组成结构见图 B.1。其中，量子信道用于传输量子态信息，经典信道用于传输除量子态以外的其他信息。

发送端由光源、调制模块、随机数发生器、数据处理模块组成。其中，调制模块的作用包括随机地对光脉冲进行强度调制来制备信号态光脉冲和诱骗态光脉冲，根据由随机数发生器输入的随机序列，对信号态光脉冲和诱骗态光脉冲进行编码信息的加载。

接收端由探测模块、解调模块、随机数发生器、数据处理模块组成。解调模块的功能包含测量基选择和量子态测量，其中测量基的选择是随机的。测量基的选择分为主动选择和被动选择，前者需要输入随机数发生器产生的随机序列，后者可以采用分束器等被动光学元件来实现。随后，探测模块对测量后的光脉冲进行探测。接收端将所选择的测量基信息通过经典信道告知发送端，发送端对量子态制备时所采用的编码基与接收端的测量基进行比对。

双方的数据处理模块通过经典信道进行对基、纠错、安全增强、鉴别等过程协商生成共享密钥。

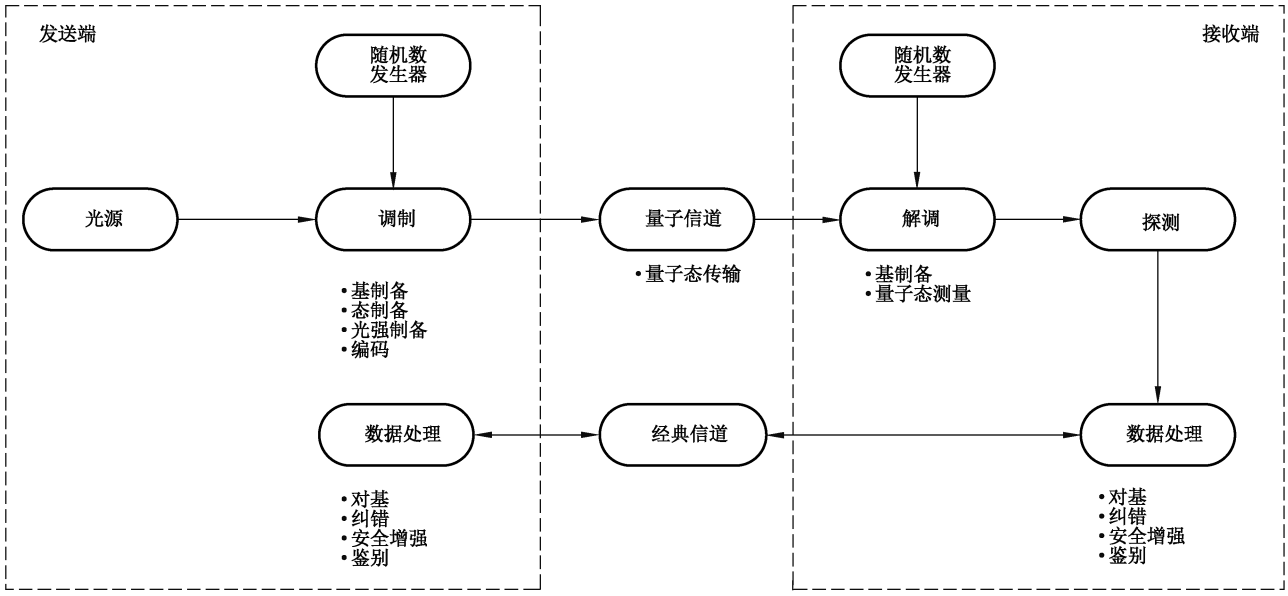

图 B.1 量子密钥分配产品的组成结构图

附 录 C
（资料性）
抵御攻击与防护措施要求

可采用的抵御攻击与防护措施的要求如下。

a） 发送端可采用输入隔离措施，以此抵御特洛伊木马攻击、激光注入攻击、种子光攻击等。

b） 接收端为主动选基方案进行量子态测量时，可采用反向隔离措施，以此抵御特洛伊木马攻击。

c） 接收端为主动选基（不选态）和被动选基方案进行量子态测量时，可采用反向隔离措施，以此抵御荧光攻击。

d） 接收端为主动选基（不选态）和被动选基方案进行量子态解码时，如果使用多个探测器，可要求同组基下的多个探测器的性能一致，包括：最大探测效率一致、门宽一致、延时扫描曲线一致、不同波长探测效率一致等，以此抵御伪造态攻击和时间位移攻击。

e） 接收端为主动选基（不选态）和被动选基方案进行量子态解码时，如果使用多个探测器，接收端在扫描延时过程后，可将多路探测器的门信号的相对延时与出厂预置的相对延时进行比较判断并具备异常告警功能，以此抵御设备校准攻击。

f） 接收端为被动选基方案进行量子态测量时，可采用弱波长相关性的基矢选择器件，或加入滤波器限制探测器的正常工作波长范围，以此抵御波长相关攻击。

g） 接收端通过多个探测器对量子态进行测量时，若同组基下的两个探测器同时响应，可采用随机选择其中之一的结果进行保留的措施，以此抵御双计数攻击。

h） 接收端通过基于 APD 的单光子探测器对量子态进行测量时，若在线性工作模式探测到信号，探测器可采用告警措施，以此抵御强光攻击。

i） 接收端通过基于 APD 的单光子探测器对量子态进行测量时，对于单探测器系统，可对 APD 的反向偏置电压检测措施，保证探测效率曲线在正常范围内；对于多探测器系统，除上述措施外，还可采用当一个探测器响应时，多探测器同时进入死时间状态的措施，以此抵御死时间攻击。

j） 接收端通过基于 APD 的单光子探测器对量子态进行测量时，可监测两个连续的探测响应时间间隔，若低于安全阈值时，则进行告警；或对探测器输出信号增加门控信号符合过滤措施，以此抵御门后攻击。

k） 接收端通过基于 APD 的单光子探测器对量子态进行测量时，可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，以此抵御雪崩过渡区攻击。

l） 接收端可采用随机数、时间戳、流水号等措施，以此抵御重放攻击。

附 录 D
（资料性）
纠错方法

D.1 概述

发送端和接收端的筛后密钥通常情况下会存在误码，需要通过纠正筛后密钥中的误码，形成纠错后密钥。纠错的原理是由通信中的一方计算并发送密钥校验信息，另一方根据校验信息对本地密钥进行迭代纠错。QKD 中常用的纠错方法主要包括 Cascade 纠错和 LDPC 纠错。其中，Cascade 纠错方法使用级联奇偶校验二分法对错误比特进行纠错，LDPC 纠错方法是使用稀疏矩阵进行校验纠错。

D.2 Cascade 纠错

Cascade 纠错方法需要多轮交互操作。假设通信双方的密钥长度为 l，并确定要进行纠错的轮数 R。具体步骤如下：

步骤 1(第 1 轮操作)：在第一轮操作中，确定分组大小为 g^1 使得每个分组内的误码个数不超过 1。通信双方将密钥分组为 $K=(k_0,k_1,\cdots,k_{g^1-1}),\cdots,(k_{l-g^1},k_1,\cdots,k_{l-1})$，记分组为$\{K_i^1\}$，$0\leqslant i\leqslant l/g^1$，计算每个分组的奇偶校验和$\{B_l^1\}$。双方比对的奇偶校验和是否相同。如果发现某个 B_l^1 不同，则代表对应分组 K_l^1 中有奇数个错误，进行二分查找，纠正误码后奇偶校验和变为相同。如果所有的$\{B_l^1\}$被纠正至相同，那么第一轮操作结束。

步骤 2(第 m 轮操作)：在第 $m(m>1)$轮操作中，双方对各自的密钥重新进行分组，分组大小为 g^m。分组是随机进行的，比特 k_i 被分到 K_j^m 是通过随机映射函数 $f(i)=j$，$0\leqslant i<l$，$0\leqslant j\leqslant l/g^m$ 进行的。分组结束后，双方分别计算奇偶校验和$\{B_i^m\}$。双方比对的奇偶校验和是否相同。如果发现某个 B_i^m 不同，则代表对应分组 K_i^m 中有奇数个误码，进行二分查找，假设找到的误码比特为 k_p。可推知在之前的所有 $m-1$ 轮操作中含有 k_p 的分组 K_i^u，$1\leqslant u<m$ 中其实含有偶数个误码未被纠正。当 k_p 被纠正后，可通过二分查找找到另一个误码并纠正。循环上面的操作，直至所有的奇偶校验和$\{B_i^m\}$均相同，则第 m 轮操作结束。

步骤 3：上述步骤进行至第 R 轮，如果此轮未纠正新的误码，则停止，否则继续下一轮直至该轮操作未纠正新的误码。

D.3 LDPC 纠错

LDPC 纠错属于经典纠错码范畴，使用稀疏矩阵作为检验矩阵进行纠错。纠错时通信双方共享校验矩阵 H(n 行 k 列)和估计的量子比特误码率，并设置最大迭代次数 N。记通信双方的 n 比特筛后密钥分别为 K_A 和 K_B。具体步骤如下：

步骤 1：发送端计算伴随式 $S_A=H*K_A$，即为矩阵与列向量乘法，并通过经典信道传送给接收端。

步骤 2：接收端根据接收到的伴随式 S_A，对本地密钥 K_B 进行迭代解码。每一轮迭代解码为 K_B'，并计算伴随式 $S_B=H*K_B'$。若 $S_A=S_B$ 相同则宣布解码成功，解码为 K_B'；否则继续迭代解码。

步骤 3：如果达到最大迭代次数 N 仍没有解码成功，则宣布解码失败并退出解码流程。

附 录 E
（资料性）
安全增强方法

E.1 安全增强方法

假设 n，m 分别为安全增强前和安全增强后的密钥长度（$n>m$）。记 $A=Z_2^n$ 和 $B=Z_2^m$ 分别为长 n 和长 m 的二元序列的集合，其中 $Z_2=\{0,1\}$ 表示二元 0/1 集合。一个杂凑函数类 $H=\{h:A\to B\}$ 如果对任意的 $x_1\neq x_2\in A$ 满足

$$|\{h\in H:h(x_1)=h(x_2)\}|\leqslant|H|/|B|$$

则称 H 是泛 2 杂凑函数类。

安全增强是通信双方通过使用泛 2 杂凑函数类来对密钥进行压缩提取。具体步骤如下：

步骤 1：确定安全增强前密钥长度 n 和安全增强后密钥长度 m，需满足 m/n 不超过压缩比 R。

步骤 2：确定需要使用的杂凑函数类 H，应当从 F.2 中选取一种。

步骤 3：由通信的一方产生选择杂凑函数所需要的随机数 r，并通过经典信道传送给通信的另一方。

步骤 4：通信双方同时根据随机数 r 选择对应的杂凑函数 $h_r:A\to B$ 来对纠错后密钥 x 进行杂凑，杂凑值 $h_r(x)$ 即为共享密钥。

E.2 常用泛 2 杂凑函数类

E.2.1 基于模算术的泛 2 杂凑函数类

定义杂凑函数类 $H_{n,m}^1=\{h_{a,b}\mid a,b\in Z_2^n,a\neq0\}$ 满足

$$h_{a,b}:A\to B$$

$$h_{a,b}(x):=[(a*x+b)\bmod 2^n]/2^{n-m}$$

其中，将 0/1 二元序列等同于整数的二进制表示。具体杂凑计算步骤如下：

步骤 1：获取两段长为 n 的二元随机序列 a，b，并准备好待杂凑的长为 n 的二元序列 x。

步骤 2：将 a，b，x 等同于二进制整数并计算 $a*x+b$。

步骤 3：截取二元序列 $a*x+b$ 中第 n 到 $n-m+1$ 位子序列，共 m 比特即为杂凑值 $h_{a,b}(x)$。

E.2.2 基本二元矩阵乘法的泛 2 杂凑函数类

一般采用特殊形式的二元矩阵—Toeplitz 矩阵来进行二元矩阵与向量乘法。由长为 $n+m-1$ 的二元序列 $s=(s_{n+m-2},\cdots,s_1,s_0)$，定义对应的 Toeplitz 矩阵为

$$T=T(s)=\begin{pmatrix}s_{n-1}&\cdots&s_1&s_0\\s_n&\ddots&\ddots&s_1\\\ddots&\ddots&\ddots&\ddots\\s_{n+m-2}&\cdots&s_m&s_{m-1}\end{pmatrix},$$

其中，T 是 m 行 n 列矩阵，且对角上的元素均相同，即 $T_{i,j}=T_{i+1,j+1}$，$0\leqslant i<m$，$0\leqslant j<n$。

定义杂凑函数类 $H_{n,m}^2=\{h_s\mid s\in Z_2^{n+m-1},s\neq0\}$ 满足

$$h_s:A\to B$$

$$h_s(x):=T(s)*x$$

其中，将二元序列等同于列向量。具体杂凑计算步骤如下：

步骤 1：获取长为 $n+m-1$ 的二元随机序列 s，并准备好待杂凑的长为 n 的二元序列 x。

步骤 2：构造 Toeplitz 矩阵 $T(s)$，计算 $T(s)*x$，即为 m 比特杂凑值 $h_s(x)$。

E.2.3 基本有限域乘法的泛 2 杂凑函数类

取 $f(t)$ 是 n 次二元不可约多项式，考虑商环 $R=Z_2[t]/<f(t)>$，其中，任意元素 $r\in R$ 可以唯一表示为低于 n 次的多项式 $r=a_0+a_1t+\cdots+a_{n-1}t^{n-1}$，其系数长 n 的二元序列 $(a_0a_1\cdots a_{n-1})\in A$，这建立了集合 R 与 A 之间的一一对应。

定义杂凑函数类 $H^3_{n,m}=\{h_r\mid r\in R\}$ 满足

$$h_r:A\rightarrow B$$

$$h_r(x):=r*x \bmod t^m$$

其中将二元序列等同商环中的元素。具体杂凑计算步骤如下：

步骤 1：获取长 n 的二元随机序列，并准备好待杂凑的长为 n 的二元序列 x。

步骤 2：计算商环乘法并表示为 $r*x=c_0+c_1t+\cdots+c_{n-1}t^{n-1}$，并截取前 m 个系数组成的长 m 的二元序列 $(c_0c_1\cdots c_{m-1})$ 即为杂凑值 $h_r(x)$。

附 录 F
（资料性）
安全增强过程中压缩比的计算公式

F.1 无限码长情况下，安全增强过程中压缩比计算公式

在无限码长情况下，安全增强过程中压缩比 R 计算公式如下：

$$R\leqslant\left\{\frac{\mu e^{-\mu}Y_1}{Q_\mu}[1-H_2(e_1)]-I_{ec}\right\};$$

上式中：

$$Y_1=\frac{\mu}{\mu\nu_1-\nu_1^2}\left[Q_{\nu_1}e^{\nu_1}-Q_u e^{\mu}\frac{\nu_1^2}{\mu^2}-Q_{v_2}\frac{(\mu^2-\nu_1^2)}{\mu^2}\right];$$

$$e_1=\min\left(\frac{E_\mu Q_\mu e^{\mu}-E_{\nu_2}Q_{\nu_2}}{Y_1\mu},\frac{E_{\nu_1}Q_{\nu_1}e^{\nu_1}-E_{\nu_2}Q_{\nu_2}}{Y_1\nu_1}\right);$$

$H_2(x)=-[x\log_2 x+(1-x)\log_2(1-x)]$为自变量 x 的二元熵函数；

$$I_{ec}=\frac{leak_{EC}}{L_{CK}};$$

$$Q_\mu=\frac{M_\mu}{N_\mu};$$

$$Q_{v_1}=\frac{\mathrm{M}_{v_1}}{\mathrm{N}_{v_1}};$$

$$Q_{v_2}=\frac{\mathrm{M}_{v_2}}{\mathrm{N}_{v_2}};$$

其中，诱骗态 2 光脉冲的平均光子数 $\nu_2\to 0$；N_μ、N_{ν_1}、N_{ν_2} 为实测参数；M_μ、M_{ν_1}、M_{ν_2} 为对基过程后统计得出；E_μ、E_{ν_1}、E_{ν_2} 为纠错过程后统计得出，见 6.2.5.2。

F.2 有限码长情况下，安全增强过程中压缩比计算公式

有限码长情况下，安全增强过程中压缩比 R 计算公式如下：

$$R\leqslant\left\{\frac{\mu e^{-\mu}Y_1^L}{Q_\mu}[1-H_2(e_1^p)]-I_{ec}\right\};$$

上式中：

$$Y_1^L=\frac{\mu}{\mu\nu_1-\nu_1^2}\left(Q_{\mathrm{v}_1}^L e^{\nu_1}-Q_u e^{\mu}\frac{\nu_1^2}{\mu^2}-Q_{v_2}^U\frac{(\mu^2-\nu_1^2)}{\mu^2}\right)$$

a) $Q_{\mathrm{v}_1}^L=\mathrm{F}_L(Q_{v_1},M_{v_1\Phi\Phi}+M_{v_1\Psi\Psi})$，其中 $Q_{v_1}=\dfrac{M_{v_1}}{N_{v1}}$；

b) $Q_{v_2}^U=\mathrm{F}_U(Q_{v_2},M_{v_2})$，其中 $Q_{v_2}=\dfrac{M_{v_2}}{N_{v_2}}$。

在计算基 Φ 单光子的相位误码率 e_1^{p} 之前，先计算基 Ψ 单光子的量子比特误码率 e_1；

$$e_1=\min\left\{\frac{E_\mu Q_\mu e^{\mu}-E_{\nu_2}Q_{v_2}^L}{Y_1^L\mu},\frac{(E_{\nu_1}Q_{\nu_1})^U e^{\nu_1}-E_{\nu_2}Q_{v_2}^L}{Y_1^L\nu_1}\right\}$$，其中：

a) $E_\mu=\dfrac{ME_\mu}{M_\mu}$，由纠错过程统计得出，见 6.2.5.2；

b) $(E_{\nu_1}Q_{\nu_1})^U=F_U(E_{\nu_1}Q_{\nu_1},ME_{v_1})$，其中 $E_{\nu_1}=\frac{ME_{v_1}}{M_{v_1}}$；

c) $Q^L_{v_2}=\max[F_L(Q_{v_2},M_{v_2}),0]$。

在无限码长情况下，基 Φ 单光子的量子比特误码率 e_1 和基 Ψ 单光子的相位误码率 e_1^p 是相同的，而在有限码长情况下，需要考虑统计涨落。假设失败概率为 ξ，基 Φ 单光子的数量为 n_Φ，基 Ψ 单光子的数量为 n_Ψ，那么，$e_1^p=e_1+\theta$，θ 值由以下的方程解得：

$$\xi=\frac{\sqrt{n_\Phi+n_\Psi}}{\sqrt{e_1^U(1-e_1^U)\,n_\Phi n_\Psi}}2^{-(n\Phi+n\Psi)\xi(\theta)}；$$

其中，$\xi(\theta)=H_2(e_1^U+\theta-q_x\theta)-q_xH_2(e_1^U)-(1-q_x)H_2(e_1^U+\theta)$，$q_\Phi=\frac{n_\Phi}{n_\Phi+n_\Psi}$；

$H_2(x)=-[x\log_2x+(1-x)\log_2(1-x)]$为自变量 x 的二元熵函数；

$$I_{ec}=\frac{leak_{\mathrm{EC}}}{L_{\mathrm{CK}}}；$$

$$Q_\mu=\frac{M_\mu}{N_\mu}；$$

$$Q_{v_1}=\frac{M_{v_1}}{N_{v_1}}；$$

$$Q_{v_2}=\frac{M_{v_2}}{N_{v_2}}；$$

其中，诱骗态 2 光脉冲的平均光子数 $\nu_2\to0$；N_μ、N_{ν_1}、N_{ν_2} 为实测参数；M_μ、M_{ν_1}、M_{ν_2} 为对基过程后统计得出；$M_{v_1\Phi\Phi}$代表发送端发送诱骗态 1 光脉冲的编码基为 Φ 时，接收端测量基同样为 Φ 时探测到的光脉冲数量；$M_{v_1\Psi\Psi}$代表发送端发送诱骗态 1 光脉冲的编码基为 Ψ 时，接收端测量基同样为 Ψ 时探测到的光脉冲数量；E_μ、E_{ν_1}、E_{ν_2} 为纠错过程后统计得出，见 6.2.5.2；函数 $F_L(p,N)a\max\left[p-\frac{1}{2}\xi(N,\varepsilon),0\right]$定义为 p 的下限，函数 $F_U(p,N)a\min\left[p+\frac{1}{2}\xi(N,\varepsilon),1\right]$定义为 p 的上限，函数 $\xi(N,\varepsilon)a\sqrt{\frac{2\ln(1/\varepsilon)+2\ln(N+1)}{N}}$，ε 代表考虑密钥有限长时统计涨落的安全参数，建议 ε 不超过 10^{-10}。

参 考 文 献

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

[2] Brassard G, Lutkenhaus N, Mor T, et al.Limitations on practical quantum cryptog-raphy [J].Physical Review Letters, 2000, 85(6):1330-1333.

[3] Brassard G, Salvail L.Secret-key reconciliation by public discussion[C].Advanc-es in Cryptology-EUROCRYPT'93.Springer Berlin Heidelberg, 1994:410-423.

[4] Chen W, Han Z F, Yin Z Q, et al.Decoy state quantum key distribution in telecom dark fiber[J]. SPIE-The International Society for Optical Engineering.2007,6827, 6282709-1.

[5] Gallager R G. Low density parity check codes [J]. IRE Transactions on Information Theory, 1962, 8(1):21-28.

[6] Gottesman D, Lo H K, Lutkenhaus N, et al.Security of quantum key distribution with imperfect devices[J].Quantum Information and Computation, 2004, 4:325-360.

[7] Han Z F, Mo X F, Gui Y Z, et al.Stability of phase-modulated quantum key distribution systems[J].Applied physics letters, 2005, 86, 221103.

[8] Hwang W Y.Quantum key distribution with high loss: toward global secure communication [J].Physical Review Letters, 2003, 91(5), 057901.

[9] Lo H K, Ma X, Chen K. Decoy state quantum key distribution [J]. Physical Review L-etters, 2005, 94(23), 230504.

[10] Lo K, Chau H F.Unconditional security of quantum key distribution over arbitrarily long distances[J].Science, 1999, 283:2050-2056.

[11] Ma X, Qi B, Zhao Y, et al.Practical Decoy State for Quantum Key Distribution[J].Physical Review A, 2005, 72(1):1-127.

[12] Mo X F, Zhu B, Han Z F, et al.Faraday-Michelson system for quantum cryptography[J]. Optics Letters, 2005, 30(19): 2632-2634.

[13] Pearson D. High-speed QKD reconciliation using forward error correction [C]. Quantum Communication, Measurement and Computing.AIP Publishing, 2004, 734(1):299-302.

[14] Wang X B. Quantum key distribution with 4 intensities of coherent light [J]. Physical Review A, 2005, 72, 012322.

[15] Wang X B, Yang L, Peng C Z, et al. Decoy state quantum key distribution with both source errors and statistical fluctuations[J].New Journal of Physics, 2009, 11,075006.

[16] Yin Z Q, Han Z F, Sun F W, et al.Decoy state quantum key distribution with modified coherent state[J].Physical Review A, 2007, 76, 014304.