



中华人民共和国国家标准

GB/T 43692—2024

量子通信术语和定义

Quantum communication terminology and definition

2024-03-15发布

2024-10-01实施

国家市场监督管理总局
国家标准化管理委员会

发布

目 次

前言 I

1 范围 1

2 规范性引用文件 1

3 通用基础术语和定义 1

4 基于光子的量子密钥分发术语和定义 7

参考文献 12

索引 13

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC485) 归口。

本文件起草单位：科大国盾量子技术股份有限公司、中国信息通信研究院、国科量子通信网络有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、数据通信科学技术研究所、安徽问天量子科技股份有限公司、中国信息通信科技集团有限公司、济南量子技术研究院、江苏亨通问天量子信息研究院有限公司、上海循态量子科技有限公司、华为技术有限公司。

本文件主要起草人：赵勇、赵梅生、敖立、张海懿、王向斌、周飞、李东东、马彰超、秦灏、程明、王海军、于宗文、刘云、刘婧婧、钱懿、赵良圆、周颖明、李政宇。

量子通信术语和定义

1 范围

本文件界定了量子通信的基本术语和定义，包括通用基础术语和定义、基于光子的量子密钥分发术语和定义。

本文件适用于量子通信技术文件的编制。

2 规范性引用文件

本文件没有规范性引用文件。

3 通用基础术语和定义

3.1

量子信息 quantum information

量子物理系统状态所包含的知识。

[来源：GB/T 42565—2023, 3.2]

3.2

经典信息 classical information

经典物理系统状态所包含的知识。

注：等价于一般意义上的信息(见GB/T4894—2009 中4.1.1.3.8和4.1.1.3.9)。

3.3

量子比特 qubit

量子信息(3.1)的最小单位，物理上用二维量子态实现，数学上可用二维希尔伯特空间的单位矢量来表示

[来源：GB/T 42565—2023, 3.3]

3.4

逻辑量子比特 logical qubit

量子信息(3.1)的最小逻辑单位，其可以处于逻辑0和逻辑1的叠加状态，数学上可用二维希尔伯特空间的单位矢量来表示。

[来源：GB/T 42565—2023, 3.5]

3.5

D 维量子位 qudit

高维的量子信息(3.1)单位，数学上可用D 维希尔伯特空间的单位矢量来表示。

3.6

量子通信 quantum communication

以量子态为信息载体，通过量子态传送实现量子信息(3.1)或经典信息(3.2)传送的技术。

注：量子通信包含多种协议方案和应用场景，如：量子密钥分发(3.9)、量子隐形传态(3.12)、量子密集编码(3.13)、量子安全直接通信(3.14)、量子秘密共享(3.15)、量子数字签名(3.16)等。

3.7

量子通信链路 quantum communication link

连接两个节点并实现量子通信(3.6)功能的物理线路。

3.8

量子通信网络 quantum communication network

由两个以上节点通过量子通信链路(3.7)连接构成的网络。

3.9

量子密钥分发 quantum key distribution;QKD

量子密钥分配

通信双方通过传送量子态的方法实现对称密钥生成的方法,在理论协议层面具备信息论安全性。

注:有多种量子密钥分发协议(4.1.1),如离散变量量子密钥分发协议(4.1.2)中的BB84协议、MDI协议、DI协议、连续变量量子密钥分发协议(4.1.3)中的GG02协议等。

3.10

量子保密通信 quantum secure communication

基于量子通信(3.6),利用量子不可分割、量子态不可克隆和量子纠缠等特性保护秘密消息,进而保证信息传输安全的通信方法。

注1:秘密消息包括密钥、口令等任何需要保护其机密性的敏感信息或数据。

注2:结合量子密钥分发(3.9)和对称密码技术的加密通信是一种典型的量子保密通信实现方案。

3.11

量子密钥 quantum key

通信双方基于量子密钥分发(3.9)协议直接生成的对称密钥,在理论协议层面可被证明具备信息论安全性。

3.12

量子隐形传态 quantum teleportation;QT

量子远程传态

一种通过对待传送的任意未知量子态和预共享量子纠缠态进行贝尔态测量,并根据测量结果对测量后的量子纠缠态进行酉变换操作以实现量子态传送的方法。

3.13

量子密集编码 quantum dense coding

一种利用预先共享的量子纠缠,仅发送一个量子比特(3.3)就可以传送多于一个比特的经典信息(3.2)的通信方法。

3.14

量子安全直接通信 quantum secure direct communication;QSDC

一种在量子信道(3.19)中用量子态编码直接传送信息,并综合利用量子态叠加、海森堡测不准关系、不可克隆定理、纠缠粒子的关联性和量子非定域性等量子力学基本原理,实现信息的安全传输的方法。

3.15

量子秘密共享 quantum secret sharing;QSS

多个通信方通过传送量子态的方法实现信息论安全的秘密共享过程。

3.16

量子数字签名 quantum digital signature;QDS

多个通信方通过传送量子态的方法实现信息论安全的数字签名的过程。

3.17

量子信号 quantum signal

量子通信(3.6)中,承载量子态的物理信号。

注1:量子通信是量子信息(3.1)的物理载体。

注2:常用的量子信号有:对偏振、相位和轨道角动量等物理量进行编码/调制的单光子、对相位和振幅进行编码/调制的弱相干态光等。

3.18

经典信号 classical signal

现代通信技术中以承载经典物理量的物理信号。

注1:是经典信息(3.2)的物理载体。

注2:常用的经典信号有,高电平、低电平、亮光脉冲、暗光脉冲、不同偏振状态的光脉冲和不同相位差的光脉冲等。

3.19

量子信道 quantum channel

传输量子信号(3.17)的信道。

3.20

经典信道 classical channel

传输经典信号(3.18)的信道。

3.21

量子态制备 preparation of quantum state(s)

操控某个物理系统,使其量子态演化或跃迁到指定量子态的过程。

3.22

偏振编码 polarization encoding

对光子或弱相干光的偏振自由度进行有限个数状态的调制。

3.23

相位编码 phase encoding

对不同时间模式,即不同时刻的光量子态的相对相位进行有限个数状态的调制。

3.24

时间-相位编码 time-bin phase encoding

对光子或弱相干光的时间模式和不同时间模式之间的相对相位进行有限个数状态的调制。

3.25

频率编码 frequency encoding

对光子或弱相干光的频率自由度进行有限个数状态的调制。

3.26

高斯调制 gaussian modulation

在连续变量量子密钥分发协议(4.1.3)中,发送方制备量子态,并且将满足高斯分布的随机数分别调制在量子态的正则分量(正则位置和正则动量)上的调制方案。

3.27

离散调制 discrete modulation

在连续变量量子密钥分发协议(4.1.3)中,发送方将随机数调制在有限个数的量子态的编码方案。

3.28

调制方差 modulation variance

调制在量子态正则分量上的随机数的方差。

3.29

单光子源 single-photon source

每次只发射出一个光子的光源。

3.30

概率性单光子源 probabilistic single-photon source

每次概率性发射单光子的光源。

3.31

纠缠对光子源 entangled-photon-pair source

发射处于量子纠缠状态的光子对的光源。

3.32

预报单光子源 heralded single-photon source

产生关联光子对，然后用其中一个光子的探测结果来预报另一个光子产生的单光子源。

3.33

诱骗态 decoy state

合法用户有意地在量子信号序列中随机插入的其他不同强度的量子信号 (3.17)。

注：诱骗态用于测试量子信道 (3.19) 是否受到攻击。

3.34

多光子信号 multi-photon signal

包含一个以上光子的脉冲信号。

3.35

平均光子数 mean photon number

每个光脉冲信号含有的光子数量的平均值。

3.36

平均光源功率 mean source power

在一个规定的时间间隔内光源的平均发光功率。

3.37

弱相干态光源 weak coherent-state source

平均光子数为单光子量级的相干光源，一般由相干激光衰减产生。

3.38

光源强度 source intensity

光源发射的光脉冲信号的平均光子数。

3.39

光子数分布 photon number distribution

每个光脉冲信号包含的光子数的概率分布。

3.40

相位随机化 phase randomization

在基于弱相干态脉冲光源的 QKD 中，发送方使弱相干态光脉冲的相位随机变化的行为。

3.41

量子态探测 detection of quantum state(s)

对某个物理系统进行量子态测量 (3.43)，并得到表示测量结果的宏观物理信号的过程。

3.42

量子态测量 quantum state measurement

对量子态进行测量以得到某个可观测物理量的值的过程。

注：量子态测量分为本征测量和非本征测量。本征测量指被测量子态是可观测物理量的本征态，测量结果是确定性的。非本征测量指被测量子态为可观测物理量多个本征态的量子叠加态，测量结果是概率性的。

[来源：GB/T 42565—2023, 3.21]

3.43

正交测量基矢 orthogonal measurement basis

一组两两互相正交的量子态，每个量子态对应某个可观测物理量的不同本征态。

3.44

单光子探测器 single-photon detector

能够以一定概率将单光子级别的光脉冲信号转化为宏观可探测信号的仪器、器件或设备。

3.45

自由运行型单光子探测器 free-running single-photon detector

工作状态下能够对任意时刻到达的光子信号进行探测的单光子探测器(3.44)。

3.46

门控型单光子探测器 gated single-photon detector

工作时通过门控信号控制有效工作时间的单光子探测器(3.44)。

注：有效工作时间也称开门时间。

3.47

上转换型单光子探测器 up-conversion single-photon detector

通过光频率上转换技术，将长波长光波段的能量低的光子变成短波长光波段的能量高的光子再进行探测的单光子探测器(3.44)。

3.48

超导单光子探测器 superconducting single-photon detector

利用超导材料的超导相变特性制作的单光子探测器(3.44)。

3.49

平衡零差探测 balanced homodyne detection

一种将待探测信号光与本振光经过平衡光分束器互相干涉，然后对两路干涉输出光做测量并求其差值以实现微弱光正则分量测量的探测方法。

注1：平衡零差探测基本原理是将与信号光与同频的本振光经过平衡光分束器干涉，对两路干涉输出光通过性能相似的线性增益光电二极管探测，利用两路测量电信号之差得到信号光正则分量测量结果。

注2：通过调节本振光和信号光之间的相位差，使用该方法可以测量信号光正则分量中的正则位置或正则动量。

3.50

本振光 local oscillator

在平衡零差探测(3.49)或双平衡零差探测(3.54)中用于与信号光进行相干干涉的相位基准信号。

3.51

随路本振光 transmitted local oscillator

在发送端生成的本振光并随量子信号光一起传输到接收端，作为信号光相干干涉的相位基准信号。

3.52

本地本振光 local local oscillator

在接收端由不同于产生信号光的激光器生成的本振光，作为信号光相干干涉的相位基准信号。

3.53

平衡零差探测器电噪声 electronic noise of homodyne detector

平衡零差探测器在接入电源后正常工作状态下，在没有任何光输入的情况下输出的电信号。

3.54

双平衡零差探测 dual balanced homodyne detection

在连续变量量子密钥分发协议(4.1.3)中,将信号光分为两束,分别通过两个本振光相位不同的平衡零差探测以测量信号光光场正则位置和正则动量的方法。

注:在连续变量量子密钥分发协议(4.1.3)中,双平衡零差探测有时也称为平衡外差探测,但其内涵与相干光通信中的外差探测方法不同。

3.55

单光子探测效率 detection efficiency

一个特定波长或频率的光子入射到单光子探测器(3.44),被探测到并输出响应信号的概率。

注:对于门控型单光子探测器(3.46),单光子探测效率指在门控时间内单光子被其探测到并输出响应信号的概率。

3.56

暗计数概率 dark count probability

在完全没有光输入时,单光子探测器(3.44)在单位时间内记录到探测事件并输出响应信号的概率。

3.57

后脉冲概率 after-pulse probability

在光子输入单光子探测器(3.44)并产生探测事件后,由于后脉冲效应导致该探测器在无光子输入的情况下错误地产生响应信号的概率。

注:后脉冲效应是指雪崩光电二极管在雪崩过程中产生的载流子被倍增层中的缺陷和杂质捕获后延迟释放并造成额外雪崩信号的现象。

3.58

死时间 dead time

单光子探测器(3.44)探测到光子信号后的状态恢复时间。

注:在死时间内,探测器对入射的单光子信号无响应。

3.59

平衡零差探测器等效探测效率 equivalent detection efficiency of homodyne detector

接收方平衡零差探测器探测到的量子光信号功率与尚未耦合进入接收方的量子光信号功率比值称为平衡零差探测器等效探测效率,反映了量子信号透过接收方的能力。

注:公式(1)如下:

$$\eta_{\text{t}}=\eta_{\text{r}}\times\eta_{\text{a}}\times\eta_{\text{m}}\quad\cdots\cdots\cdots(1)$$

式中:
 η_{m} ——平衡零差探测器等效探测效率;
 η_{r} ——接收端损耗;
 η_{om} ——平衡零差探测器效率;
 η_{m} ——模式匹配效率。

3.60

散粒噪声 shot noise

对于平衡零差探测器电噪声(3.53)为零时的理想情况,在只有本振光(3.50)输入而无信号光输入时的零差探测输出信号。

注:散粒噪声来源于真空态涨落。

3.61

散粒噪声单位 shot noise unit

散粒噪声(3.60)的强度的统计方差。

3.62

散粒噪声极限 shot noise limit

散粒噪声单位(3.61)大于平衡零差探测器电噪声强度的统计方差的情况。

3.63

量子随机数 quantum random number

基于量子力学原理所保证的随机性过程产生的真随机数

注：量子力学原理所保证的随机性过程包括但不限于：量子态测量的非本征测量过程，真空态涨落引起的自发辐射初始相位以及真空态测量涨落等。

3.64

量子随机数发生器 quantum random number generator;QRNG

产生量子随机数(3.63)的器件。

4 基于光子的量子密钥分发术语和定义

4.1 协议和方案

4.1.1

量子密钥分发协议 QKD protocol

量子密钥分配协议

基于量子力学的基本原理保证通信双方之间能够生成一串完全相同且攻击者无法获取信息的随机数以作为共享密钥的方法和过程。

注：量子密钥分发协议规定的关键过程包括：(1)编码发送，将发送方数据编码成为量子信号通过量子信道送出；(2)解码探测，接收方对量子信号进行解码和探测得到接收方数据；(3)密钥协商，需要进行密钥分发的双方在经过认证的公开信道上交互不涉及秘密信息的数据，通过纠错和保密增强(4.1.16)协商出双方一致的安全密钥。

4.1.2

离散变量量子密钥分发协议 discrete variable QKD protocol;DV-QKD

利用本征矢量族有限可数的量子态(如单光子的偏振态、相位态、时间-相位态，或双光子纠缠态等)进行密钥分发的协议。

注：离散变量量子密钥分发协议的安全性由量子力学的单光子不可分割、测不准定理和不可克隆定理等特性保证。

4.1.3

连续变量量子密钥分发协议 continuous variable QKD protocol;CV-QKD

利用拥有连续变量特征的光场量子态(如压缩态、相干态、双模压缩态等)进行密钥分发的协议。

注：连续变量量子密钥分发协议的安全性由量子力学的海森堡测不准定理等特性保证。

4.1.4

设备无关量子密钥分发 device-independent QKD;DI-QKD

基于量子力学非定域性，利用量子纠缠进行 QKD 的过程和方案。

注：设备无关量子密钥分发安全性不依赖于对量子态制备和测量设备的安全性假设。

4.1.5

测量设备无关量子密钥分发 measurement-device-independent QKD;MDI-QKD

一种安全性不依赖于对量子态测量设备的安全性假设的QKD 方案。

4.1.6

半设备无关量子密钥分发 semi-device-independent QKD;SDI-QKD

一种安全性仅依赖于量子制备和测量设备状态的希尔伯特空间维度数限定假设的 QKD 方案。

4.1.7

诱骗态方案 decoy-state scheme

在 DV-QKD 协议(4.1.2)中，采用多种随机的光强来监测信道并估计单光子的量子态特性，从而解

决非理想单光子光源的安全漏洞并提高量子密钥分发(3.9)效率的一种光源实现方案。

4.1.8

原始密钥 raw key

在QKD 密钥协商(4.1.9)过程中,成功测量到的量子信号的对应位置上的发送方数据和接收方数据。

4.1.9

密钥协商 key reconciliation

通信双方通过公共认证经典信道进行信息交互,对原始密钥(4.1.8)进行处理从而获得相同密钥的过程。

4.1.10

正向协商 direct reconciliation

在QKD 密钥协商(4.1.9)中,接收方以发送方的密钥为基准,将己方密钥纠正与发送方相同的密钥协商(4.1.9)的方法。

4.1.11

反向协商 reverse reconciliation

在 QKD 密钥协商(4.1.9)中,发送方以接收方的密钥为基准,将己方密钥纠正与接收方相同的密钥协商(4.1.9)的方法。

4.1.12

筛选 sifting

在 QKD 密钥协商(4.1.9)中,合法通信双方对量子信号进行测量后,通过公开信息的通信对原始密钥(4.1.13)进行挑选的过程。

注:当公开信息中只有测量基矢信息被用于挑选原始密钥(4.1.8)时,此过程也称为对基。

4.1.13

筛选后密钥 sifted key

在 QKD 密钥协商(4.1.9)中,原始密钥经过筛选(4.1.12)后所得到的密钥。

4.1.14

参数估计 parameter estimation

在 QKD 密钥协商(4.1.9)中,对筛选后密钥统计并公布部分统计数据以获得纠错和保密增强(4.1.16)过程中所需参数的过程。

4.1.15

纠错后密钥 corrected key

在 QKD 密钥协商(4.1.9)中,筛选后密钥(4.1.13)去除被公布的数据后,所剩余部分经过纠错后所得到的密钥。

4.1.16

保密增强 privacy amplification

隐私放大

密性增强

安全增强

在 QKD 密钥协商(4.1.9)中,通信双方根据QKD 安全理论方案计算获得的压缩率,将纠错后密钥(4.1.15)进行压缩,将窃听者获得的信息量减少至可以忽略的水平以得到安全的最终密钥的过程。

4.1.17

最终密钥 final key

纠错后密钥(4.1.15)经过保密增强(4.1.16)后所得到的密钥。

4.1.18

片协商 slice reconciliation

在连续变量量子密钥分发协议(4.1.3)中,将连续变量进行量化分层,使得连续变量量化成多个离散变量,再通过公共认证经典信道交互信息,利用纠错码译码纠错使得通信双方共享一致密钥的密钥协商方法。

4.1.19

多维协商 multidimensional reconciliation

在连续变量量子密钥分发协议(4.1.3)中,将服从高斯分布的 d 个连续变量组合成 d 维矢量,并随机映射到 d 维单位球面上约定矢量集合中的某一个,然后通过公共认证经典信道交互信息,利用纠错码译码纠错使得通信双方共享一致密钥的密钥协商方法。

4.2 组网和网元

4.2.1

量子密钥分发网络 quantum key distribution network;QKDN

基于QKD,实现指定用户间安全的密钥分发功能的网络。

4.2.2

量子密钥分发设备 QKD device

实现QKD功能的设备,包括接收端和发送端。

4.2.3

量子密钥分发链路 QKD link

连接两个QKD设备之间的通信链路,用以完成量子密钥分发过程。

4.2.4

密钥管理 key management

量子密钥分发设备(4.2.2)产生量子密钥(3.11)之后的量子密钥生命周期中,对量子密钥执行的全部操作。

注:密钥管理包括密钥的存储、格式化、中继、将密钥提供给应用程序、根据策略或协议规定对密钥进行保留或删除等操作。

4.2.5

密钥管理器 key manager;KM

布设在QKD节点的用以实现量子密钥管理功能的设备。

4.2.6

密钥管理链路 KM link

连接KM的通信链路,用以完成密钥管理过程。

4.2.7

量子密钥分发网络控制器 QKDN controller

量子密钥分发网络中用以实现量子密钥分发网络控制功能的功能实体。

4.2.8

量子密钥分发网络管理器 QKDN manager

量子密钥分发网络中用以实现对量子密钥分发网络的监视和管理功能的功能设备。

4.2.9

用户网络 user network

密码应用程序使用由量子密钥分发(QKD)网络提供的密钥的一种网络。

4.2.10

量子密钥分发系统 QKD system

在两个或两个以上通信节点间，利用量子密钥分发设备通过光纤或自由空间信道完成安全的最终密钥分发的系统。

4.2.11

量子信道的光交换 optical switch for quantum channel

通过光纤量子信道的交换连接，实现多台QKD 设备互连的设备。

4.2.12

可信中继 trusted relay

采用一个可信任的中继节点，该节点的设备和存储不会被非法方控制和侵入，与另外两个或多个合法通信节点分别进行 QKD，由此实现所连节点之间的密钥共享从而拓展 QKD 安全成码距离和范围的一种技术。

4.2.13

量子中继 quantum repeater

在远距离量子通信时，用于克服量子信道噪声和衰减的影响，保持量子态量子特性并提高量子态传输效率的中继设备。

注：量子中继的方法原理主要有两类。第一类方法基于量子存储，并通过分段的量子纠缠分发、量子纠缠交换与量子纠缠纯化相结合的方式实现远距离的高品质量子纠缠分发，再利用远距离量子纠缠实现量子通信。第二类方法则利用量子容失编码和量子纠错编码，分段对量子信号进行恢复，实现远距离的量子通信。量子中继用于拓展 QKD安全成码距离和范围。

4.2.14

量子信道复用 quantum channels multiplexing

将多个量子信道在同一根光纤中按照不同自由度进行复用的技术。

示例1：使用同一光纤中不同时间隙内的光量子信号实现不同量子信道的复用。

示例2：使用同一光纤中不同波长上的光量子信号实现不同量子信道的复用。

4.2.15

量子-经典信道复用 multiplexing of quantum channel(s) and classical channel(s)

将量子信道与经典信道在同一根光纤中按照不同自由度进行复用的技术。

示例1：使用同一光纤不同时间隙内的量子信号或经典信号实现量子信道与经典信道复用。

示例2：使用同一光纤不同波长上的光量子信号和经典信号实现量子信道与经典信道复用。

4.2.16

星地量子密钥分发 satellite-to-ground QKD

在卫星平台上的节点和地面节点之间，以自由空间作为量子信道进行 QKD 的技术。

4.3 性能指标

4.3.1

最终成码速率 final key rate

安全成码率 secure key rate

单位时间内QKD 系统生成的最终密钥的数量。

注1：多使用统计平均值，常用单位有：比特每秒(bps)、千比特每秒(kbps)和兆比特每秒(Mbps)。

注2：也可用平均每发送一个量子信号所生成最终密钥数量来定义最终成码速率。

4.3.2

最大安全成码距离 maximum secure distance

在满足一定最终成码速率(4.3.1)要求时 QKD 系统容忍的最大信道衰减所对应的光纤/自由空间

量子信道的长度。

注：对应不同类型的光纤，单位长度衰减可能不等，相同的最大信道衰减对应的最大安全成码距离也可能各不相同。

4.3.3

量子比特误码率 quantum bit error rate; QBER

量子比特错误率

在 DV-QKD 协议 (4.1.2) 中，筛选后密钥 (4.1.13) 发生比特错误的比率。

4.3.4

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。

注：在 QKD 的安全性分析中，该数值被用于估计窃听者知晓的密钥信息量。

4.3.5

工作频率 operating frequency

一个 QKD 系统工作时，单位时间内发送量子信号 (3.17) 的数量。

注：工作频率和 QKD 系统最终成码速率 (4.3.1) 的上限相关。

4.3.6

信道传输率 channel transmission

透过信道进入接收方还未进行探测的量子光信号功率与发送方发出进入信道介质时量子光信号功率的比值。

注：信道传输率反映了量子信号透过信道介质的能力。

4.3.7

过噪声 excess noise

CV-QKD 系统噪声中除系统散粒噪声之外的部分，由系统不完美性、信道噪声或信道窃听引入。

4.3.8

协商效率 reconciliation efficiency

在连续变量量子密钥分发协议 (4.1.3) 中，纠错后密钥信息量减去密钥协商中通过公共认证经典信道交互的信息量后与筛后密钥互信息量的比值称之为协商效率。

4.4 安全性

4.4.1

失败概率 failure probability

实际的 QKD 设备在完成 QKD 的过程中，所生成的密钥被具有无限计算资源和任意计算能力的窃听者攻击获取的最大概率。

注：失败概率也可等价地使用量子迹距离刻画。

4.4.2

量子黑客攻击 quantum hacking

利用 QKD 设备器件的性能或功能缺陷，增加 QKD 过程中量子信息的泄漏量，从而获取 QKD 安全密钥的攻击方法。

参 考 文 献

- [1] GB/T4894—2009 信息与文献 术语
- [2] GB/T 42565—2023 量子计算 术语和定义
- [3] Л.н. 朗道, Е.М. 栗弗席兹, Л.н.Ландау, 等. 量子力学：非相对论理论[M]. 高等教育出版社, 2008.

索引

汉语拼音索引

A	
暗计数概率	3.56
B	
半设备无关量子密钥分发	4.1.6
保密增强	4.1.16
本地本振光	3.52
本振光	3.50
C	
参数估计	4.1.14
测量设备无关量子密钥分发	4.1.5
超导单光子探测器	3.48
D	
D维量子位	3.5
单光子探测器	3.44
单光子探测效率	3.55
单光子源	3.29
多光子信号	3.34
多维协商	4.1.19
F	
反向协商	4.1.11
G	
概率性单光子源	3.30
高斯调制	3.26
工作频率	4.3.5
光源强度	3.38
光子数分布	3.39
过噪声	4.3.7
H	
后脉冲概率	3.57

J	
经典信道	3.20
经典信号	3.18
经典信息	3.2
纠缠对光子源	3.31
纠错后密钥	4.1.15
K	
可信中继	4.2.12
L	
离散变量量子密钥分发协议	4.1.2
离散调制	3.27
连续变量量子密钥分发协议	4.1.3
量子安全直接通信	3.14
量子保密通信	3.10
量子比特	3.3
量子比特误码率	4.3.3
量子黑客攻击	4.4.2
量子-经典信道复用	4.2.15
量子秘密共享	3.15
量子密集编码	3.13
量子密钥	3.11
量子密钥分发	3.9
量子密钥分发链路	4.2.3
量子密钥分发设备	4.2.2
量子密钥分发网络	4.2.1
量子密钥分发网络管理器	4.2.8
量子密钥分发网络控制器	4.2.7
量子密钥分发系统	4.2.10
量子密钥分发协议	4.1.1
量子数字签名	3.16
量子随机数	3.63
量子随机数发生器	3.64
量子态测量	3.42

量子态探测	3.41
量子态制备	3.21
量子通信	3.6
量子通信链路	3.7
量子通信网络	3.8
量子信道	3.19
量子信道的光交换	4.2.11
量子信道复用	4.2.14
量子信号	3.17
量子信息	3.1
量子隐形传态	3.12
量子中继	4.2.13
逻辑量子比特	3.4

M

门控型单光子探测器	3.46
密钥管理	4.2.4
密钥管理链路	4.2.6
密钥管理器	4.2.5
密钥协商	4.1.9

P

偏振编码	3.22
片协商	4.1.18
频率编码	3.25
平衡零差探测	3.49
平衡零差探测器等效探测效率	3.59
平衡零差探测器电噪声	3.53
平均光源功率	3.36
平均光子数	3.35

R

弱相干态光源 3.37

S

散粒噪声	3.60
散粒噪声单位	3.61

散粒噪声极限	3.62
筛选	4.1.12
筛选后密钥	4.1.13
上转换型单光子探测器	3.47
设备无关量子密钥分发	4.1.4
失败概率	4.4.1
时间-相位编码	3.24
双平衡零差探测	3.54
死时间	3.58
随路本振光	3.51

T

调制方差	3.28
------------	------

x

相位编码	3.23
相位误码率	4.3.4
相位随机化	3.40
协商效率	4.3.8
信道传输率	4.3.6
星地量子密钥分发	4.2.16

Y

用户网络	4.2.9
诱骗态	3.33
诱骗态方案	4.1.7
预报单光子源	3.32
原始密钥	4.1.8

Z

正交测量基矢	3.43
正向协商	4.1.10
自由运行型单光子探测器	3.45
最大安全成码距离	4.3.2
最终成码速率	4.3.1
最终密钥	4.1.17

英文对应词索引

A

after -pulse probability3.57

B

balanced homodyne detection3.49

C

channel transmission4.3.6

classical channel 3.20

classical information3.2

classical signal 3.18

continuous variable QKD protocol 4.1.3

corrected key4.1.15

D

dark count probability3.56

dead time 3.58

decoy state3.33

decoy-state scheme4.1.7

detection efficiency 3.55

detection of quantum state (s)3.41

device-independent QKD4.1.4

direct reconciliation4.1.10

discrete modulation3.27

discrete variable QKD protocol4.1.2

dual balanced homodyne detection 3.54

E

electronic noise of homodyne detector3.53

entangled -photon -pair source3.31

equivalent detection efficiency of homodyne detector3.59

excess noise 4.3.7

F

failure probability4.4.1

final key rate4.3.1

final key4.1.17

free-running single-photon detector3.45

frequency encoding 3.25

G

gated single-photon detector3.46

gaussian modulation3.26

H

heralded single-photon source3.32

K

key management4.2.4

key manager(KM)4.2.5

key reconciliation4.1.9

KM link 4.2.6

L

local oscillator 3.50

logical qubit3.4

M

maximum secure distance4.3.2

mean photon number3.35

mean source power 3.36

measurement-device-independent QKD4.1.5

modulation variance 3.28

multi -photon signal3.34

multiplexing of quantum channel(s)and classical channel(s)4.2.15

O

operating frequency 4.3.5

optical switch for quantum channel4.2.11

orthogonal measurement basis3.43

P

parameter estimation4.1.14

phase encoding3.23

phase error rate4.3.4

phase randomization 3.40

photon number distribution3.39

polarization encoding3.22

preparation of quantum state(s)3.21

privacy amplification 4.1.16

probabilistic single-photon source3.30

Q

QKD device **4.2.2**

QKD link 4.2.3

QKD protocol 4.1.1

QKD system **4.2.10**

QKDN controller 4.2.7

QKDN manager 4.2.8

quantum bit error rate **4.3.3**

quantum channel **3.19**

quantum channels multiplexing **4.2.14**

quantum communication link 3.7

quantum communication network **3.8**

quantum communication 3.6

quantum dense coding **3.13**

quantum digital signature **3.16**

quantum hacking 4.3.2

quantum information **3.1**

quantum key 3.11

quantum key distribution **3.9**

quantum key distribution network 4.2.1

quantum random number **3.63**

quantum random number generator 3.64

quantum repeater 4.2.13

quantum secret sharing 3.15

quantum secure communication 3.10

quantum secure direct communication **3.14**

quantum signal 3.17

quantum state measurement **3.42**

quantum teleportation 3.12

qubit 3.3

qudit **3.5**

R

raw key 4.1.8

reconciliation efficiency **4.3.8**

reverse reconciliation 4.1.11

S

satellite-to-ground QKD **4.2.16**

semi-device-independent QKD 4.1.6

shot noise 3.60

shot noise limit **3.62**

shot noise unit3.61

sifted key4.1.13

sifting4.1.12

single-photon detector 3.44

single-photon source3.29

slice reconciliation4.1.18

source intensity3.38

superconducting single-photon detector 3.48

T

time-bin phase encoding3.24

transmitted local oscillator3.51

trusted relay4.2.12

U

up-conversion single-photon detector3.47

user network4.2.9

W

weak coherent-state source3.37

