



中华人民共和国国家标准化指导性技术文件

GB/Z XXXXX—XXXX

量子随机数发生器量子熵源测试规程

Code of practice for testing quantum entropy sources in quantum random number
generators

（征求意见稿）

（本草案完成时间：2026.7.6）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 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	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 量子熵源结构组成及工作原理	2
4.1 结构组成	2
4.2 工作原理	2
5 要求	3
5.1 量子随机过程要求	3
5.2 可测试性要求	3
5.3 一致性与稳定性要求	3
5.4 随机源序列的采集检测与最小熵评估	3
6 测试方法	4
6.1 测试接口	4
6.2 通用测试环境与准备	4
6.3 量子随机过程机理审查	5
6.4 可测试性确认	5
6.5 一致性与稳定性测试	5
6.6 随机源序列的采集检测与最小熵评估	6
附录 A（资料性） 不同熵源技术方案工作原理	7
A.1 相位涨落方案	7
A.2 真空涨落方案	7
A.3 ASE 噪声方案	8
A.4 多光子态方案	9
A.5 电子隧穿方案	9
附录 B（资料性） 不同 QRNG 方案补充测试项目	11
B.1 相位涨落 QRNG	11
B.2 真空涨落 QRNG	11
B.3 ASE 噪声 QRNG	11
B.4 多光子态 QRNG	12
B.5 电子隧穿 QRNG	12
参考文献	13

前 言

本文件为规范类指导性技术文件

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。

本文件由全国量子技术标准化技术委员会（SAC/TC 578）归口。

本文件起草单位：合肥国家实验室、中国科学技术大学、济南量子技术研究院、国科量子通信网络有限公司、中国科学院软件研究所、中国电子科技网络信息安全有限公司、中国人民解放军网络空间部队信息工程大学、中国信息通信研究院、科大国盾量子技术股份有限公司、中电信量子信息科技集团有限公司、安徽问天量子科技股份有限公司、上海循态量子科技有限公司、武汉光谷信息光电子创新中心有限公司、武汉量子技术研究院、中移量子科技有限公司、中国信息安全测评中心、中国计量科学研究院、中国标准化研究院、中国科学院计算技术研究所、香港大学、太原理工大学、宁波大学、中国长城科技集团股份有限公司、江苏省计量科学研究院、山东省体育彩票管理中心。

本文件主要起草人：聂友奇、吴佳颖、张军、张强、白冰、江扬帆、李明翰、陈华、徐兵杰、周淳、赖俊森、郑明睿、王超凡、刘慧、姜艳、李东东、黄溢智、刘婧婧、李华生、华昕、韩玄、魏瑛、刘宏伟、邓玉强、张萌、周泓伊、张行健、郭晓敏、陈超、于春霖、赵品彰、刘宁。

量子随机数发生器量子熵源测试规程

1 范围

本文件描述了量子随机数发生器量子熵源结构组成及工作原理，提供了量子随机数发生器量子熵源的要求和测试规程。

本文件适用于量子随机数发生器中量子熵源部分的测试。

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 25069—2022 信息安全技术 术语

GB/T 43692—2024 量子通信术语和定义

3 术语和定义

GM/T 0103—2021、YD/T 6445—2025以及GB/T 43692—2024中界定的下列术语和定义适用于本文件。

3.1

熵源 entropy source

产生输出的部件、设备或事件。当该输出以某种方法捕获和处理时，产生包含熵的比特串。

[来源：GM/T 0103—2021, 3.1]

3.2

量子熵源 quantum entropy source

基于量子力学原理所保证的随机性过程产生输出的部件、设备或事件，其输出是包含熵的随机信号。

[来源：YD/T 6445—2025, 3.1]

3.3

量子随机过程 quantum random process

具有内禀量子随机性的随机现象/过程。

注：其随机性质由量子力学原理解释和保证。用于产生随机数的量子随机过程一般包括：单光子路径选择、光脉冲所包含的光子数、相邻光子间时间间隔、真空涨落、激光相位噪声、放大自发辐射噪声等。

[来源：GM/T 0103—2021, 3.5，有修改]

3.4

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。

[来源：GB/T 43692—2024, 3.63]

3.5

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

产生量子随机数（3.4）的器件。

[来源：GB/T 43692—2024, 3.64]

3.6

随机源序列 raw random number sequence

熵源输出经数字化得到的离散随机值序列。

[来源：GM/T 0103—2021, 3.8]

3.7

随机数序列 random number sequence
数列中的每一项在已知其他项的情况下都无法被推断的一种数列。
[来源：GM/T 0103—2021, 3.9]

4 量子熵源结构组成及工作原理

4.1 结构组成

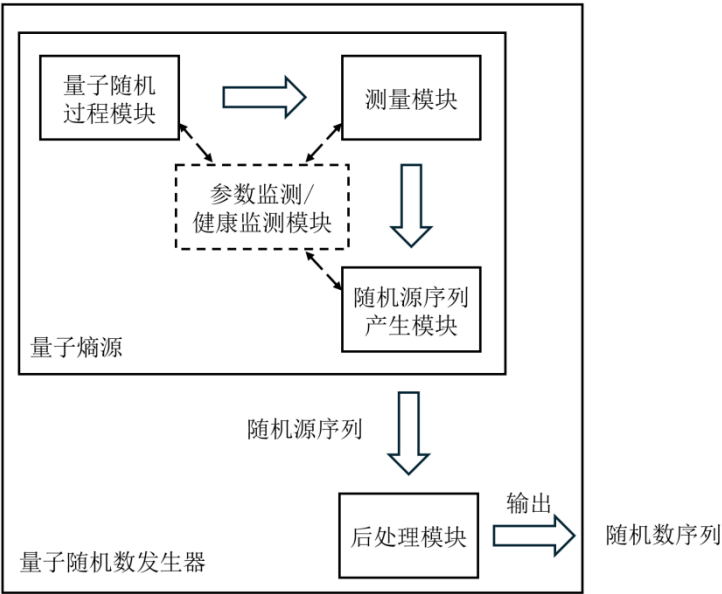


图1 量子随机数发生器以及其中的量子熵源基本架构

量子随机数发生器量子熵源的典型技术方案可包括相位涨落、真空涨落、放大自发辐射（Amplified Spontaneous Emission, ASE）噪声、多光子态和电子隧穿等，相关技术方案可参考YD/T 6445—2025。量子熵源作为量子随机数发生器（QRNG）的核心组件，主要由量子随机过程模块、测量模块、随机源序列产生模块、参数监测/健康监测模块组成，其基本架构见图1。一个完整量子随机数发生器主要包括量子熵源以及后处理模块。量子熵源内部包括量子随机过程模块、测量模块、随机源序列产生模块，以及可选的参数监测/健康监测模块；后处理模块不属于量子熵源。

4.2 工作原理

根据图1所示的架构，测量模块将量子随机过程产生的随机性转换为可观测的物理信号；随机源序列产生模块对测量输出的模拟信号、事件信号、时间标记或计数结果等进行采集、转换或记录，形成后处理前的随机源序列。随机源序列产生模块仅指形成随机源序列所必需的采集转换环节，可包括 模数转换器（Analog-to-Digital Converter，ADC）、时间-数字转换器（Time-to-Digital Converter，TDC）、比较器、计数器或事件记录单元等，具体边界应结合熵源模型、测试接口和产品设计文件确定。参数监测/健康监测模块用于对量子随机过程模块、测量模块和随机源序列产生模块的关键工作参数、状态信息和必要的随机源序列统计特性进行监测。后处理模块不属于量子熵源本体，其输入为随机源序列，输出为随机数序列。

其基本工作原理如下：

- a) 量子随机过程模块产生具有内禀量子随机性的物理状态、事件或变量；
- b) 测量模块对量子随机过程对应的量子态、事件或变量进行测量，将量子随机性转换为可观测的物理信号；
- c) 随机源序列产生模块对测量输出的模拟信号、事件信号、时间标记或计数结果等进行采集、转换或记录，形成后处理前的随机源序列；
- d) 随机源序列输入后处理模块，经随机性提取、压缩或去偏等处理后，输出随机数序列。

参数监测/健康监测模块用于对熵产生过程中的关键环境变量、工作参数和运行状态进行监测。该模块可根据具体实现方式设置，不改变随机源序列与随机数序列之间的前后处理关系。目前主要的量子随机数发生器中量子熵源的工作原理，见附录A。

5 要求

5.1 量子随机过程要求

量子熵源应满足以下要求：

- a) 基于量子随机过程：量子熵源应基于至少一个量子随机过程，确保其随机性源于量子力学内禀特性；
- b) 可证明的量子随机性：量子随机过程贡献的随机性应有明确的理论模型，并结合熵源模型、经典噪声贡献和适用的侧信息假设，给出随机源序列中量子随机成分的最小熵下界；适用时，可给出条件最小熵下界。

5.2 可测试性要求

量子熵源应具备可测试性，具体包括：

- a) 标准化测试接口：应提供物理测试接口，支持对量子随机过程模块、测量模块及随机源序列产生模块的检测；
- b) 参数监测/健康监测能力：量子熵源宜集成实时参数监测/健康监测模块，确保关键工作参数（适用时可包括光源输出功率、探测器性能参数、器件温度、随机源序列健康监测等）可被持续监测。

5.3 一致性与稳定性要求

量子熵源的实际实现状态应与设计文件、熵源模型及安全分析保持一致，用于熵评估的随机源序列应能够代表设计预期下的量子随机过程，避免因组件、通道、采集位置或工作条件不一致而影响熵估计和安全结论的有效性。量子熵源一致性与稳定性要求包括：

- a) 熵源关键组件一致性要求：量子熵源关键组件的类型、型号、参数范围、连接关系和工作条件应与设计文件、熵源模型及适用的安全分析一致。
对于光学型量子熵源，适用时可包括激光器、发光器件、单光子源、光衰减器、分束器、调制器等组件的相关参数；对于非光学型量子熵源，适用时可包括隧穿器件、散粒噪声器件、放射性衰变源、自旋噪声源、偏置电路、放大电路等组件的相关参数。
- b) 物理通道一致性要求：与量子随机过程产生、传输、耦合、调制或转换有关的物理通道应与设计文件和熵源模型一致。对于光学型量子熵源，适用时可包括干涉路径差、相位关系、偏振状态、光功率分配、耦合关系等参数；对于非光学型量子熵源，适用时可包括偏置条件、阻抗匹配、频率响应、噪声耦合路径、屏蔽与接地方式等参数。
- c) 测量结果采集链路一致性要求：随机源序列产生模块及其相关链路应与熵源输出信号特性相匹配。适用时，其带宽、增益、输入范围、采样率、分辨率、阈值设置、动态范围等参数应满足随机源序列生成和最小熵评估的要求。
- d) 随机源序列输出接口一致性要求：随机源序列输出接口、采集位置、数据格式、采样位宽、采样速率或时间分辨率、数据记录方式等应与测试方案和设计文件一致。对于含有后处理或随机性提取模块的设备，随机源序列采集位置和随机数序列输出位置应明确区分。
- e) 多通道或多熵源结构一致性要求：对于包含多个熵源、多路采集通道或并行随机数生成通道的设备，各通道的关键组件、物理通道、采集链路和数据合并方式应与设计文件一致。适用时，各通道应分别满足本条所列一致性要求。
- f) 稳定性要求：量子熵源应在规定工作条件下保持关键参数和输出特性的稳定。稳定性评价对象可包括与熵源模型相关的物理参数、采集参数、输出速率和随机源序列统计特性等。

测试项目、测试点和判定依据应根据量子随机数发生器的熵源类型、系统架构、熵源模型和产品设计文件确定。

5.4 随机源序列的采集检测与最小熵评估

量子熵源应能够说明随机源序列中包含可定量评估的量子随机性。量子熵源应基于随机源序列以及熵源模型相匹配的分析方法，给出随机源序列中量子随机成分的最小熵下界。最小熵下界的确定不宜以“完全避免经典噪声混入”作为判据，而应识别、估计并约束经典噪声对熵评估的影响，确保采用的随机性下界主要来源于量子随机成分。

量子熵源随机源序列的采集与检测应保证后续分析的完整性、可追溯性和可靠性，主要包括：

- a) 数据采集：测评平台应通过标准化接口接入量子熵源设备，调用其驱动级数据采集模块，获取并归档随机源序列，为后续分析与检测提供数据基础。
- b) 数据检测：应基于采集到的随机源序列开展分布特性分析、最小熵评估和必要的健康检测或失效检测。随机源序列不宜以通过随机数序列随机性检测作为判定依据。
 - 1) 分布特性分析：应对随机源序列开展分布特性分析及必要的统计检验，验证其是否与熵源模型及量子随机过程的理论预期相一致。分布特性分析可用于快速判断熵源输出质量，并为异常状态识别、一致性验证和后续熵评估提供依据。
 - 2) 最小熵评估：应依据适用的熵评估方法，对随机源序列中的量子随机成分贡献的最小熵下界进行评估，作为后处理模块提取比例设置的依据。

6 测试方法

6.1 测试接口

测试接口应结合图1所示量子熵源结构设置，并能够区分量子随机过程模块、测量模块、随机源序列产生模块与后处理模块。对于采用 ADC、TDC、比较器、计数器或事件记录单元等采集转换环节的量子熵源，应明确随机源序列采集位置及相关采集参数；相关采集转换环节对信号的影响宜纳入熵源模型和最小熵评估。对于含有后处理或随机性提取模块的设备，应分别确认随机源序列采集位置和随机数序列输出位置。参考测试接口见图2。

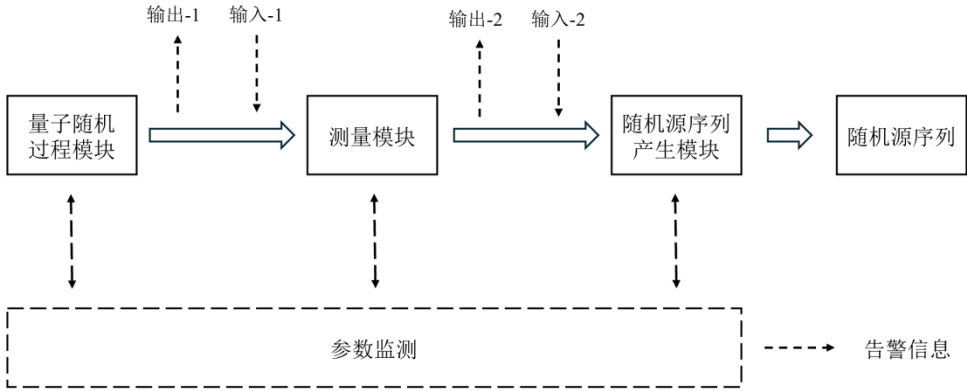


图2 量子熵源测试接口

图2中参考测试接口说明如下：

- 输出-1：用于检测量子随机过程模块的输出状态；
- 输入-1：用于向测量模块输入外部标准参考量子态或参考变量；
- 输出-2：用于检测测量模块的输出信号特性；
- 输入-2：用于向随机源序列产生模块输入外部标准参考信号。

6.2 通用测试环境与准备

测试环境、测试设备、测试软件和测试接口应根据被测量子熵源类型、系统架构、测试项目和产品设计文件确定。测试环境应记录温度、湿度等可能影响测试结果的条件；对于开放式光学结构或对环境敏感的设备，还应记录洁净度、气流和光学平台状态等条件。

测试设备应根据测试项目和被测参数确定，其量程、带宽、采样率、时间分辨率、准确度和校准状态等应满足测试要求。用于定量测量的测试设备应在有效校准期间内，其不确定度等指标应满足相应测

试项目的要求，并在测试方案或测试记录中说明。可使用的测试设备包括但不限于计算机、光功率计、光电探测模块、示波器、频谱仪、信号源、环境监测设备和数据采集设备。具体设备及其技术指标应在测试方案和测试记录中明确。

测试软件可由集成化测试平台或分立软件工具组成，应支持数据采集、参数记录、数据存储、熵评估、统计分析和结果导出等功能。

测试前应完成以下准备工作：

- a) 记录测试环境条件；
- b) 核查被测设备、测试设备、软件版本、连接方式和测试数据采集位置；
- c) 记录被测设备型号、硬件版本、固件版本和关键工作参数；
- d) 确认设备驱动、数据采集程序和数据保存路径正常；
- e) 根据测试方案配置被测设备，使其进入稳定工作状态；
- f) 对于多通道或多熵源结构，明确各通道编号、采集位置和数据合并方式。

6.3 量子随机过程机理审查

量子随机过程审查应通过文件审查、模型核查和必要的物理量测试，确认被测熵源随机性来源是否与声明的量子随机过程相一致，并确认其满足5.1规定的要求。必要的物理量测试可根据熵源类型和声明的量子随机过程确定，适用时可包括光功率、相位关系、干涉可见度、探测器响应、噪声方差、光子计数、事件发生率、时间间隔分布、偏置电压、电流、温度等参数测试。具体测试项目可结合产品设计文件、熵源模型和附录B中不同QRNG方案的补充测试项目确定。

6.4 可测试性确认

可测试性确认应确认被测熵源是否具备开展后续测试所需的接口、数据、文档和参数监测能力，并确认其满足5.2规定的要求。可测试性确认内容宜包括：

- a) 核查测试接口位置、接口类型、连接方式、访问权限和数据读取方式；
- b) 核查随机源序列采集位置、数据格式、采样位宽、采样速率或时间分辨率、样本导出方式等信息；
- c) 核查产品说明、设计文件、熵源模型、接口说明、采集程序或驱动说明等文件是否能够支持测试实施；
- d) 适用时，核查关键工作参数、参数监测、健康监测、异常告警或状态记录功能是否可读取或导出；
- e) 必要时，通过采集样本数据或读取状态信息，验证接口、数据采集和记录功能是否正常。

6.5 一致性与稳定性测试

一致性与稳定性测试应根据熵源类型和设计文件，对关键组件、物理通道、测量结果采集链路、输出接口、多通道结构以及长期运行状态进行核查或测量，并确认其满足5.3规定的要求。对于不同QRNG方案，除本条通用测试项目外，还可结合附录B给出的补充测试项目开展一致性与稳定性测试。

- a) 关键组件一致性测试：核查关键组件的类型、型号、参数范围、连接关系和工作条件；适用时，测量光功率、偏置电压、电流、探测器响应、放大链路增益、频率响应等关键组件参数。测试结果宜与设计文件、熵源模型和产品说明一致。
- b) 物理通道一致性测试：根据熵源类型确定需要测试的物理通道参数；对光学型量子熵源，适用时测试干涉路径差、相位关系、偏振状态、光功率分配、耦合关系等；对非光学型量子熵源，适用时测试偏置条件、阻抗匹配、频率响应、噪声耦合路径、屏蔽与接地方式等。测试结果宜与设计文件和熵源模型一致。
- c) 测量结果采集链路一致性测试：核查探测、放大、滤波、比较、采样和模数转换或时间数字转换等链路配置；适用时，测试或核查带宽、增益、输入范围、采样率、分辨率、阈值设置和动态范围等参数。被测信号带宽与采样率或时间分辨率、输入幅度与动态范围、阈值设置与信号分布之间宜相匹配。
- d) 输出接口一致性测试：核查随机源序列采集位置、接口类型、数据格式、采样位宽、采样速率或时间分辨率和记录方式；采集样本数据并解析数据格式，确认数据来源和记录方式与测试方

案一致。对于含有后处理或随机性提取模块的设备，宜分别确认随机源序列采集位置和随机数序列的输出位置。

- e) 多通道或多熵源结构测试：对于包含多个熵源、多路采集通道或并行随机数生成通道的设备，宜分别核查各通道关键组件、物理通道、采集链路和数据合并方式。各通道测试结果及数据合并方式宜与设计文件一致。
- f) 稳定性测试：在规定工作条件下连续运行被测设备，按照测试方案设定监测周期和采样间隔，记录与熵源模型相关的关键物理参数、采集参数、输出速率和随机源序列统计特性；必要时绘制波动曲线并计算平均值、方差、极差、漂移量等统计指标。测试结果宜表明关键参数和输出特性在测试期间保持稳定，且未出现影响最小熵评估有效性的异常漂移。适用时，可根据产品设计文件、应用场景或相关环境试验要求，开展温度循环、长时间连续运行等环境适应性或稳定性验证。

6.6 随机源序列的采集检测与最小熵评估

随机源序列的采集检测与最小熵评估宜结合熵源模型、产品设计文件、测试方案及适用的熵评估方法开展。测试时宜在后处理前的随机源序列采集位置获取样本，记录采集位置、接口类型、数据格式、采样位宽、采样速率或时间分辨率、样本长度及相关工作参数；适用时，还宜结合关键工作参数、随机源序列统计特性、输出速率、异常告警状态等开展健康检测或失效检测，用于识别熵源工作状态异常或随机源序列分布显著偏离熵源模型的情况。

本文件中的随机性下界主要指随机源序列中量子随机成分贡献的最小熵下界；适用时，可包括条件最小熵下界。最小熵评估可基于随机源序列及熵源模型开展，说明随机源序列中量子随机成分、经典噪声成分及其他非理想因素之间的关系，并结合熵源模型、器件工作参数、参考输入或基线测试、噪声方差、事件率或分布参数估计等方式，分析经典噪声对评估结果的影响。适用时，可结合分布特性分析、IID/Non-IID判断或其他统计分析结果确定熵评估方法，并在测试记录中说明样本长度、参数设置、评估结果和判定依据。相关随机源序列熵评估思路可参考 YD/T 6445—2025，最小熵概念及IID/Non-IID熵评估思路可参考 NIST SP 800-90B。后处理后随机数序列的随机性检测可按 GM/T 0005—2021 等相关规范开展，不作为本条随机源序列最小熵评估的判定依据。

测试记录或评估结果宜包括：

- a) 随机源序列采集位置、接口类型、数据格式、样本长度及采集参数；
- b) 随机源序列分布特性分析结果，以及适用时的 IID/Non-IID 判断结果；
- c) 量子随机成分、经典噪声成分及其他非理想因素的分析或约束说明；
- d) 采用的熵评估方法、参数设置、最小熵下界、置信水平或适用条件；
- e) 健康检测或失效检测结果，以及异常数据处理说明；
- f) 后处理模块提取比例确定依据。

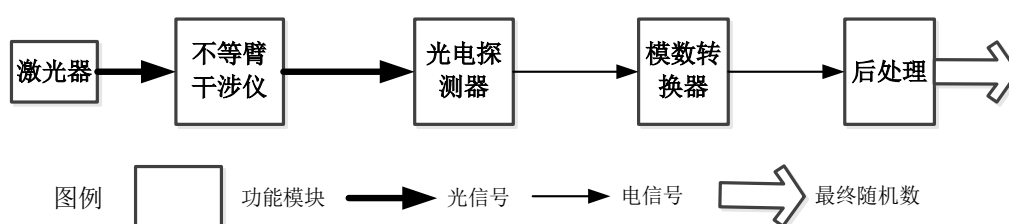
附录 A

(资料性)

不同熵源技术方案工作原理

A.1 相位涨落方案

相位涨落QRNG主要结构见图A.1, 包括激光器、干涉仪、光电探测器、模数转换器。其中激光器设置在临界状态上, 以保证自发辐射光子的比例占优势; 干涉仪通过光的干涉将输入激光信号中的相位涨落转化为强度涨落, 可以是马赫-曾德干涉仪、法拉第旋转镜干涉仪或者光纤环等; 光电探测器对光信号的强度进行探测, 输出模拟电信号; 模数转换器将连续的模拟电信号转化为原始数字信号。对于模数转换器输出的随机源序列, 还要经过一个后处理过程将其转化为无偏的随机数序列。



图A.1 基于相位涨落的量子随机数发生器基本结构

相位涨落量子随机数发生器的随机性来自于激光器内部介质的自发辐射带来的随机相位涨落。激光器内部工作介质的原子能级跃迁会产生两种辐射, 受激辐射和自发辐射。后者由真空涨落引起, 发射出的光子相位具有高度的随机性。相位涨落量子随机数发生器的功能是将这种自发辐射的随机相位提取出来产生随机数。

激光器的泵浦电流存在一个阈值, 低于这个阈值, 激光器内部仅存在微弱的自发辐射, 无激光输出, 高于此阈值时才会有输出, 随着泵浦电流增大, 受激辐射将成为主导。量子随机数发生器工作时, 将泵浦电流强度设为略高于阈值, 这样可以使激光器输出中自发辐射的比例尽可能高。

光电探测器输出的电信号中同时包含量子信号与经典噪声, 其定量关系由 (A.1) 式表示:

$$\sigma_V^2 = A_Q P + A_C P^2 + F \dots \dots \dots (A.1)$$

式中:

σ_V^2 ——光电探测器输出电信号的方差, 单位为 V^2 ;

A_Q ——与量子噪声贡献相关的一次项拟合系数, 单位为 V^2/W ;

A_C ——与功率相关经典噪声贡献相关的二次项拟合系数, 单位为 V^2/W^2 ;

P ——激光器输出功率, 单位为 W ;

F ——与激光器输出功率无关的经典噪声方差项, 单位为 V^2 。

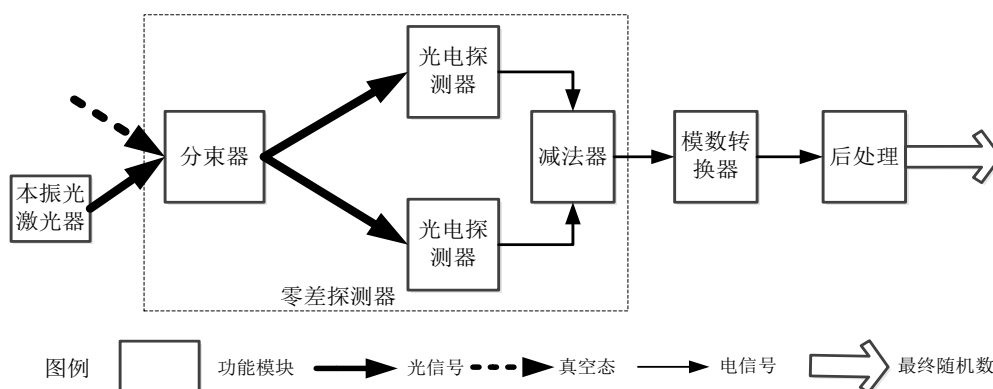
第一项 $A_Q P$ 为量子信号, 后两项 $A_C P^2 + F$ 为经典噪声。公式 (A.1) 表明, 量子信号与经典噪声和激光器功率 P 均有关。可以看出经典电信号的方差是 P 的二次函数, 各项系数 A_Q , A_C , F 可以通过拟合的方式计算出来。通过改变 P 的值, 即可改变量子信号与经典噪声的比例, 设置一个适当的 P 值可以使这一比例达到最大, 量子随机数的产生过程便在这个功率下进行。

根据所使用的制备和测量方案, 量子信号测量结果可能呈高斯分布或者其他分布。通过测出总信号的方差可以计算出量子信号的方差, 进而根据理论分布计算出测量值的最大可能概率 P_{max} , 随后可根据最小熵公式计算出模数转化后得到的随机源序列的量子随机成分的最小熵值, 根据该熵值即可以设置后处理的提取参数, 提取出无偏的随机数序列。

A.2 真空涨落方案

真空涨落QRNG是一种连续变量随机数发生器, 通过对真空态进行零差探测, 将其结果作为随机数的随机源序列。真空涨落QRNG结构如图A.2所示, 主要由本振光激光器、零差探测器、模数转换器和

后处理模块组成。零差探测器是经典相干光通信中常用器件，内部结构包括一个分束器，用于信号光和本振光的干涉；两个光电探测器，将光强起伏转化为光电流；减法器，输出两路光电流的差值。本振光是一束强相干光，作为输入待测信号光的参考光。通过调节本振光的相位可以改变其与信号光的相对相位，从而实现对信号光不同正则分量的测量。在真空涨落量子随机数发生器中，输入的信号光为真空态，真空态在相空间中是各向同性的，即测量真空态光场的不同正则分量会得到相同的统计结果，因此不需要刻意调节本振光的相位。



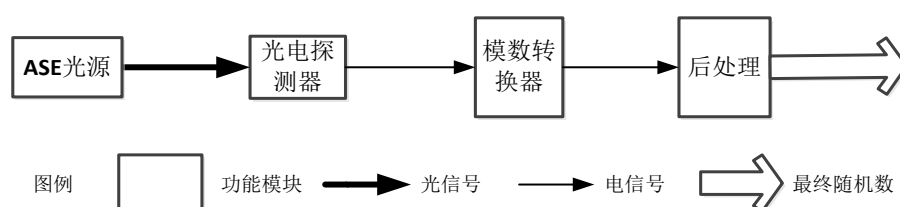
图A.2 基于真空涨落的量子随机数发生器基本结构

真空涨落量子随机数发生器的测量结果中会包含量子噪声和经典噪声。量子噪声在本振光的光强很强的条件下近似服从高斯分布；经典噪声一般为电子器件引入的噪声，一般认为与量子噪声是彼此独立的，也近似服从高斯分布。因此测量结果是两个独立的高斯分布的叠加，总方差满足 $\sigma_t^2 = \sigma_Q^2 + \sigma_C^2$ ，等式右边分别是量子信号和经典噪声的方差。其中前者可以被本振光的光强放大，而后者不能被放大，是一个常数。因此可以通过改变本振光的光强来标定经典噪声的强度。

真空涨落量子随机数发生器随机性的最小熵值可通过拟合或统计的方法来计算。零差探测的测量结果，也就是模数转换器的输入是一个高斯分布的连续信号，最大概率 P_{max} 通常取决于高斯分布概率密度函数在模数转换器中间帧、MSB和LSB三帧中积分面积最大的一个。以一个刻度均匀的模数转换器为例，最大概率就是高斯分布概率密度函数在模数转换器最中间的刻度内的面积。当然，可以通过合理设置模数转换器的刻度区间，使得高斯分布概率密度函数在每个区间内的面积相等，这样模数转换器输出的数字信号便具有相对较大的最小熵。

A.3 ASE 噪声方案

放大自发辐射（ASE）噪声是一种广泛存在于光纤通信系统中的现象，例如利用掺铒光纤放大器（EDFA）或半导体光放大器对信号光进行放大时，除受激辐射效应之外，不可避免地会产生自发辐射，自发辐射信号经过增益介质后得到放大即产生ASE噪声信号。ASE噪声是一种典型的量子效应，其信号幅值体现出真随机性。



图A.3 基于放大自发辐射的量子随机数发生器

ASE噪声QRNG如图A.3所示，主要由ASE光源、光电探测器、模数转换器和后处理组成。ASE光源模块输出放大自发辐射光量子噪声信号，通常由超辐射发光二极管（SLED）构成；光电探测器用于实现对SLED输出的ASE噪声进行光电变换，将ASE光噪声信号转换为易于采集处理的模拟电噪声信号；

ADC器件将光电探测器输出的模拟电信号转换为离散化随机源序列；数据后处理提取随机源序列的随机性，得到随机数序列。

光电探测器（PD）对ASE光信号进行直接探测，得到与ASE光场强度成正比的光电流信号，而ASE光场强度与PD实际探测到的光子数成正比，因此探测输出的光电流大小应正比于ASE光场实际被探测到的光子数目，二者在理论上具有一致的统计特性。因此，可认为ASE噪声信号的随机性源自于其光子数分布的随机性。ASE光场可用多模热场态来进行等价建模。当ASE光场包含M个独立模式时，其光子数的统计分布是这M个模式统计分布的卷积，也就是著名的玻色-爱因斯坦分布，由式（A.2）表示。

$$P(\bar{n}, n, M) = \frac{\Gamma(n+M)}{\Gamma(n+1)\Gamma(M)} \left(1 + \frac{1}{\bar{n}}\right)^{-n} (1 + \bar{n})^{-M} \dots\dots\dots (A. 2)$$

式中：

M——总模式数

$\bar{n}$ —— PD 探测时间窗口内每个模式的平均光子数。 $\Gamma x=0+\infty tx-1e^{-t}dt(x>0)$

$$\Gamma(x) = \int_0^{+\infty} t^{x-1} e^{-t} dt \quad (x > 0)$$

，当x为正整数时，可以证明伽玛函数 $\Gamma x=x-1!$ 。当n、 $\bar{n}$ 和M均为正整数时，玻色-爱因斯坦分布的等价表达形式如式（A.3）所示。

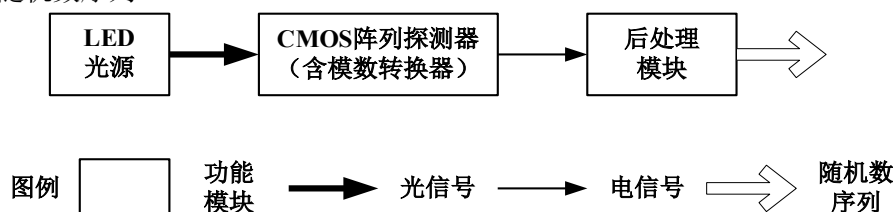
$$P(\bar{n}, n, M) = \frac{(n+M-1)!}{n!(M-1)!} \left(1 + \frac{1}{\bar{n}}\right)^{-n} (1 + \bar{n})^{-M} \dots\dots\dots (A. 3)$$

当模式数M增大时，该分布渐进收敛于高斯分布。上述光子数分布的ASE光场经光电探测后即可得到正比于光场光子数的高斯分布随机信号。

ASE噪声QRNG的测量结果中通常包含量子噪声和经典噪声，两者相互独立且都服从高斯分布。在已知两者方差之比的条件下，可量化计算观测结果中仅由量子噪声所引起最小熵。基于该最小熵估计，结合数据后处理方法，可提取出无偏的随机数序列。

A. 4 多光子态方案

多光子态QRNG如图A.4所示。LED光源模块由恒流源驱动处于低光强输出工作状态，经过特定光路结构后由CMOS阵列探测器进行光电信号探测转换。LED发出光子数目在短时间尺度上具有随机性，同时CMOS阵列探测器不同像素捕获光子响应事件也具有随机性，二者共同构成多光子态QRNG量子熵源的随机过程。CMOS阵列探测器输出经过放大和模数转换之后的随机源序列，在后处理模块中进行数据压缩，输出随机数序列。



图A. 4 基于多光子态的 QRNG

多光子态QRNG的测量结果中包含量子噪声和经典噪声。量子噪声来源于LED光源在单位时间内随机发射的光子数，服从泊松分布；经典噪声来源于探测器模块内部所包含的噪声，包括热噪声、暗电流以及读出电路噪声等，一般认为它们与量子噪声是彼此独立的并服从高斯分布。因此测量结果是两者的叠加。

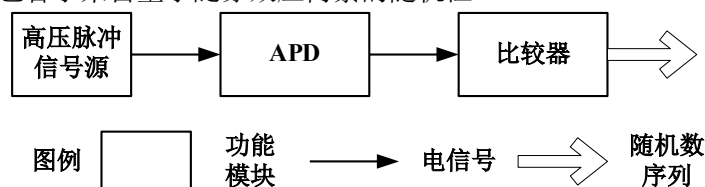
当CMOS传感器的探测光子数和输出数字值的转换增益大于等于1时，量子噪声的随机性可以通过平均值为N的泊松分布的最小熵来计算，其中N为CMOS探测器探测的平均光子数，其计算公式如式（A.4）所示：

$$H_{min} = -\log_2 \left(\max(P_q) \right) = -\log_2 \left(\frac{e^{-N} N^N}{N!} \right) \dots\dots\dots (A. 4)$$

通过计算探测器探测到的平均光子数，可以评估随机源序列中量子噪声的随机性。

A. 5 电子隧穿方案

一种典型的电子隧穿QRNG如图A.5所示,包括高压脉冲信号、雪崩光电二极管(APD)、比较器。其中雪崩光电二极管由高压脉冲信号进行驱动。在未施加高压脉冲时,雪崩光电二极管处于较低偏压的复位状态;当施加脉冲时,雪崩光电二极管内有一定概率出现电子隧穿并产生隧穿电信号。隧穿电信号输入到比较器,由比较器通过阈值判别法判断隧穿事件的发生,获取隧穿事件发生的相关信息作为随机源序列。随机源序列包含了来自量子隧穿效应内禀的随机性。



图A.5 基于电子隧穿的 QRNG

电子隧穿效应是典型的量子效应。当固体内势垒宽度较窄时,电子有一定概率穿过高于自身能量的势垒从势垒一端到达另一端,形成隧穿电流。在单位时间内,电子是否发生隧穿或发生隧穿的电子个数均体现出量子随机性。二极管内电子发生隧穿的概率可由式(A.5)所示描述:

$$f = \frac{kTm_{eff}}{2\pi^2\hbar^3} \times \int_{\varepsilon_{min}}^{\varepsilon_{max}} TC(\varepsilon_x) \ln \left(\frac{1 + \exp\left(\frac{\varepsilon_{Fn} - \varepsilon_x}{kT}\right)}{1 + \exp\left(\frac{\varepsilon_{Fn} - \varepsilon_x - qV}{kT}\right)} \right) d\varepsilon_x \dots\dots\dots (A.5)$$

式中:

f ——二极管单位时间内发生隧穿的平均电子个数

k ——玻尔兹曼常数

T ——绝对温度

m_{eff} ——电子有效质量

ε_x ——电子在沿势垒方向的能量

ε_{Fn} —— n 区电子费米能

q ——电子电荷量

V ——二极管两端电压

$TC(\varepsilon_x)$ ——对应能量电子的传输系数,该系数由二极管结构、掺杂浓度等因素决定。

在量子力学中,测量引起波函数的塌缩,塌缩具有量子内禀的真随机性。因此通过测量量子隧穿效应事件可以获得量子随机性。一般采用单位时间内电子隧穿事件的有无或电子隧穿事件发生的时间来获取随机源序列。

在电子隧穿事件有无的方案中,可通过调节二极管两端电压 V ,实现在一个脉冲时间内,阈值判别二极管内电子发生与不发生隧穿事件的概率比为50:50,发生隧穿事件记为1/0,不发生隧穿事件记为0/1,由此输出随机源序列。

在电子隧穿事件发生时间的方案中,单光子探测器在过偏压的情况下可以通过量子隧穿效应形成暗计数,可采用时间数字转换器测量单光子探测器暗计数的发生时间,实现随机源序列的输出。采取死时间设计抑制后脉冲后,可以假设每个时间间隔之间的暗计数事件是独立的。假设单个时间窗口内发生暗计数的概率为 p ,那么暗计数发生在第 k 个时间窗口应当满足概率见公式(A.6):

$$p(T = k) = (1 - p)^{k-1}p \dots\dots\dots (A.6)$$

附录 B (资料性) 不同 QRNG 方案补充测试项目

B.1 相位涨落 QRNG

相位涨落QRNG的补充测试项目宜在第6章通用测试方法基础上，结合激光器、干涉仪、光电探测器、模数转换器以及随机源序列采集位置确定。

- a) 原理与模型审查：核查产品说明文档、原理图、必要的光学设计图、硬件电路图、固件或 FPGA 逻辑说明，确认被测熵源基于相位涨落量子随机过程，且熵源模型、关键组件和采集位置与测试方案一致。
- b) 光源稳定性测试：在规定工作状态下，通过光功率计或等效测试设备监测激光器输出功率，记录平均值、标准差、均方根波动等指标，并与设计文件或标称值进行比对。
- c) 干涉链路测试：适用时测试不等臂干涉仪臂长差、相位关系和相位维稳状态，确认臂长差避开采样周期或其整数倍，且干涉输出满足熵源模型要求。
- d) 测量输出统计特性测试：在干涉输出端、光电探测器输出端或放大后信号端采集数据，分析幅度分布、均值、方差、带宽和异常漂移，必要时开展正态性或其他模型匹配检验。
- e) 采集与转换链路测试：核查光电探测器、放大器、滤波器和模数转换器的带宽、输入范围、采样率、分辨率和动态范围，确认被测信号带宽与采样率之间的匹配关系。
- f) 量子噪声与经典噪声贡献评估：可通过改变激光器功率、引入等效参考光或采用拟合方法，估计量子涨落和经典噪声对总方差的贡献，并将评估结果用于最小熵或随机性下界分析。
- g) 随机源序列检测：在后处理前的随机源序列输出位置获取样本，开展分布特性分析、熵评估和必要的健康检测，确认测试数据能够代表相位涨落熵源的原始输出。

B.2 真空涨落 QRNG

真空涨落QRNG的补充测试项目宜围绕本振光、分束器、平衡零差探测器、模数转换器和随机源序列采集链路开展。

- a) 原理与模型审查：核查被测设备是否采用真空态输入与本振光进行零差探测的方案，确认真空态输入、分束器、两个光电探测器、减法或平衡探测链路及数据采集位置与熵源模型一致。
- b) 本振光稳定性测试：记录本振光功率、波长、偏振状态和工作稳定性等参数，确认其处于设计规定的有效工作范围。
- c) 分束器分光比测试：适用时分别测量分束器两个输出端口的光功率，计算分光比并与设计要求或标称值进行比对。
- d) 探测器一致性测试：测量两个光电探测器的响应度、输出电流或等效响应参数，确认其一致性满足零差探测和噪声抵消要求。
- e) 零差探测输出测试：在零差探测器放大后输出端采集信号，测试输出幅度分布、方差、带宽和漂移情况，并与真空涨落模型预期进行比对。
- f) 模数转换输出测试：采集模数转换器输出的随机源序列，核查采样率、分辨率、采样区间和数据格式，分析随机源序列分布是否符合模型预期。
- g) 量子噪声与经典噪声分离评估：可通过改变本振光强并记录输出方差，采用拟合方法估计经典电子噪声和量子噪声贡献，形成最小熵评估的输入依据。

B.3 ASE 噪声 QRNG

ASE噪声QRNG的补充测试项目宜围绕ASE光源、光电探测器、采集链路、经典噪声控制和随机源序列熵评估开展。

- a) 原理与模型审查：核查 ASE 光源类型、增益介质、探测方式、模数转换链路和后处理前随机源序列输出位置，确认随机性来源于放大自发辐射噪声并具有相应的理论模型。
- b) ASE 光源状态测试：记录 ASE 光源输出功率、光谱范围、工作电流或驱动条件及其稳定性，确认其处于设计规定的工作区间。

- c) 光电探测链路测试：核查光电探测器的带宽、响应范围、饱和状态、放大链路增益和模数转换器采样参数，确认采集链路能够覆盖 ASE 噪声信号的有效带宽和幅度范围。
- d) 分布特性测试：采集光电探测后或模数转换后的随机源序列，依据熵源模型分析其统计分布；当模型预期为多模热场近似或高斯近似时，宜开展相应的模型匹配检验。
- e) 经典噪声评估：通过关闭或阻断 ASE 光源、调整光源功率或采集电子噪声基线等方式，估计探测器和采集链路引入的经典噪声，并分析其对最小熵估计的影响。
- f) 随机源序列熵评估：基于随机源序列和量子噪声贡献估计结果，计算随机性下界，并记录后处理参数与熵评估结果之间的对应关系。

B.4 多光子态 QRNG

多光子态QRNG的补充测试项目宜围绕发光器件、探测阵列、光子计数或像素响应模型、经典噪声和采集链路开展。

- a) 原理与模型审查：核查 LED 或其他发光器件、光路结构、CMOS 或等效探测阵列、放大与模数转换链路，确认随机性来源于光子数或探测事件的量子统计涨落。
- b) 光源与工作条件测试：记录发光器件驱动电流、光强、曝光时间、温度等工作参数，确认其处于低光强或设计规定的有效工作范围。
- c) 探测阵列测试：核查探测阵列的响应均匀性、暗电流、读出噪声、转换增益、饱和情况和坏点处理方式，确认采集结果不会由固定图样噪声或读出链路异常主导。
- d) 统计分布测试：采集后处理前的像素响应、光子计数或数字采样形成的随机源序列，分析其是否符合泊松分布、近似高斯分布或设计文件声明的统计模型。
- e) 经典噪声与背景扣除评估：通过暗场、遮光或固定输入条件测试估计热噪声、暗电流和读出电路噪声，分析其对量子随机成分和最小熵评估的影响。
- f) 随机源序列与多通道一致性测试：对于多像素、多区域或多通道结构，分别记录各通道统计特性和数据合并方式，必要时比较通道间一致性并开展熵评估。

B.5 电子隧穿 QRNG

电子隧穿QRNG的补充测试项目宜围绕隧穿器件、偏置条件、比较或时间测量链路、死时间设计、隧穿事件分布和熵评估开展。

- a) 原理与模型审查：核查雪崩光电二极管、单光子雪崩二极管、隧穿二极管或其他隧穿器件的结构、偏置方式、阈值判别或时间数字转换链路，确认随机源序列来源于电子隧穿相关事件。
- b) 偏置与触发条件测试：记录脉冲幅度、反向偏压、脉冲宽度、重复频率、温度和阈值设置，确认器件工作在设计规定的隧穿事件采集状态。
- c) 事件分布测试：根据方案类型采集隧穿事件有无、事件计数或发生时间数据，分析其是否符合几何分布、泊松分布、二项分布或设计文件声明的统计模型。
- d) 阈值与概率平衡测试：对于采用事件有无生成比特的方案，宜测试阈值设置、电压调节和事件发生概率，确认随机源序列偏置处于设计允许范围。
- e) 死时间与后脉冲影响测试：核查死时间设置、恢复时间和后脉冲抑制措施，评估相邻事件之间的相关性及其对独立同分布假设和熵评估的影响。
- f) 随机源序列健康检测与熵评估：适用时开展重复计数检测、自适应比例检测、分布特性分析和最小熵评估，并记录评估方法、样本长度、误报率或判定阈值。

参 考 文 献

- [1] GM/T 0103—2021 随机数发生器总体框架
 - [2] GM/T 0005—2021 随机性检测规范
 - [3] YD/T 6445—2025 量子随机数发生器技术规范
 - [4] NIST SP 800-90B: 2018 Recommendation for the Entropy Sources Used for Random Bit Generation
-