

《量子随机数发生器量子熵源测试规程》

国家标准化指导性技术文件编制说明

(征求意见稿)

2026 年 7 月

目 录

一、工作简况	1
（一）任务来源及协作单位	1
（二）制定背景	1
（三）主要工作过程	2
（四）国家标准主要起草人及其所做的工作	7
二、国家标准编制原则、主要内容及其确定依据	10
（一）标准编制原则和依据	10
（二）标准主要技术内容说明	10
（三）标准中主要技术内容确定的依据和过程	11
三、试验验证情况的说明	15
（一）主要试验的分析	15
（二）主要试验验证的分析、综述报告	15
（三）试验方案设计	16
（四）试验结果	16
四、与国际、国外同类标准技术内容的对比情况	16
五、标准采用国际文件的情况说明	18
六、与有关的现行法律、法规和强制性国家标准的关系	19
七、制修订过程中是否存在重大分歧意见，以及重大分歧意见的处理过程	19
八、标准中涉及专利的情况	19
九、国家标准性质的建议及贯彻国家标准的要求和措施建议	19
十、其他应予说明的事项	20

《量子随机数发生器量子熵源测试规程》 国家标准化指导性技术文件编制说明

一、工作简况

（一）任务来源及协作单位

本标准由全国量子技术标准化技术委员会（SAC/TC 578）提出并归口管理，起草单位包括合肥国家实验室、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等。其中，合肥国家实验室为该标准起草工作的牵头单位。

（二）制定背景

在国家顶层布局和相关部委的大力支持下，我国量子信息技术整体处于国际领先地位，其中量子密钥分发和量子随机数技术在实用化方面发展最为突出，正处于从技术领先向产业综合领先发展的关键时期，急需标准化工作的指导。特别在中共中央、国务院于2021年10月印发的《国家标准化发展纲要》中，将“推动标准化与科技创新互动发展”放在五大任务之首，提出要加强关键技术领域标准研究，以科技创新提升标准水平，健全科技成果转化标准的机制。《纲要》明确指出，要“在人工智能、量子信息、生物技术等领域，开展标准化研究……部分领域关键标准适度领先于产业发展平均水平。”

量子随机数发生器是一种利用量子力学效应产生随机数的设备，其应用范围包括科学模拟、密码学等。本指导性技术文件项目聚焦于量子随机数发生器中核心的量子熵源，清晰的定

义其通用技术要求，并计划给出参考测试方法，提供全面的设计与测评指南，推动量子随机数发生器产品的研制以及测评，从而促进量子随机数在量子通信等相关领域中的应用和发展。

（三）主要工作过程

2025 年 1 月 4 日，合肥国家实验室联合中国科学技术大学、济南量子技术研究院、国科量子通信网络有限公司成立前期工作组，启动《量子随机数发生器量子熵源检测规范》标准的起草准备工作；2025 年 6 月 26 日，前期工作组向全国量子技术标准化技术委员会（TC578）提交了标准的立项申报资料；2025 年 10 月 14 日，前期工作组向全国量子技术标准化技术委员会（TC578）提交了修改后的标准立项申报资料，并将标准文件的类型更改为指导性技术文件，名称更改为《量子随机数发生器量子熵源测试规程》；2025 年 11 月 11 日全国量子技术标准化技术委员会（TC578）全体委员投票表决通过立项。

2025 年 11 月 13 日，完成国家标准化指导性技术文件登记，由 TC578（全国量子技术标准化技术委员会）归口，主管部门为国家标准委。项目登记名称《量子随机数发生器量子熵源测试规程》，登记号：20256263-Z-469，任务周期 12 个月。任务下达后，技术归口单位全国量子技术标准化技术委员会，会同项目牵头单位合肥国家实验室，面向领域内相关科研院所、企事业单位、社会团体等，广泛开展了标准起草工作组成员单位/起草专家的征集工作。

2026 年 3 月 31 日，《量子随机数发生器量子熵源测试规程》

指导性技术文件起草工作组正式成立。起草工作组由来自合肥国家实验室、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及山东省体育彩票管理中心共25个单位的32名专家构成。聂友奇任组长，组员有吴佳颖、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、赵品彰及刘宁。

2026年3月31日，国家标准计划《量子随机数发生器量子熵源测试规程》第一次起草工作组会议以线上方式召开。会议由牵头立项单位合肥国家实验室聂友奇主持，国科量子通信网络有限公司、科大国盾量子技术股份有限公司、上海循态量子科技有限公司、山东省体育彩票管理中心、中国科学院计算技术研究所、安徽问天量子科技股份有限公司、合肥国家实验室、

宁波大学、香港大学、中国电子科技网络信息安全有限公司、中电信量子信息科技集团有限公司、中国信息通信研究院、济南量子技术研究院、中国科学院软件研究所、中国计量科学研究院等 15 家单位的 22 位专家出席。会议介绍了标准立项及前期工作情况、项目周期和工作计划，对整体草案进行了逐条解读，并围绕量子熵源边界、原始数据采集/数字化部分是否纳入量子熵源、术语定义、量子熵源结构、可测试性、一致性与稳定性、最小熵评估、测试章节结构及测试报告等内容开展讨论。会议明确会后通过工作群和邮件收集专家正式反馈，由起草组整理会议纪要、意见汇总处理表和修改稿。第一次会议形成修改意见 26 条。

2026 年 4 月至 6 月，工作组对第一次会议形成的 26 条意见进行了逐条研究和处理，重点对文件名称及相关表述、规范性引用文件、术语定义、量子熵源结构边界、数字化/原始数据采集模块定位、测试章节结构、结果判别和测试报告等内容进行了修改完善，形成修改后的草案，并将相关材料发送工作组成员征求进一步意见。

2026 年 6 月 16 日，国家标准计划《量子随机数发生器量子熵源测试规程》第二次起草工作组会议以线上方式召开。会议由牵头立项单位合肥国家实验室聂友奇主持，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、武汉量子技术研究院、中国信息安全测评中心、中国标准化研究院、中国计量科学研究院、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、中国人民解放军网络空间部队信息工程大学、中移量子科技有限公司、武汉光谷信息光电子创新中心有限公司、中国长城科技集团股份有限公司、中科酷原科技（武汉）有限公司、山东省体育彩票管理中心、江苏省计量科学研究院等 24 家单位的 30 位专家出席。会议回顾了第一次会议纪要及意见处理情况，介绍了标准起草工作进展、工作计划和当前草案修改情况，并对草案内容再次进行逐条讨论。与会专家重点围绕标准题名和英文名称、全文术语统一、规范性引用文件适用性、量子随机过程表述、量子熵源边界及原始数据采集定位、测试设备通用要求、量子随机过程审查、一致性与稳定性测试、随机源序列采集检测与最小熵评估、附录中不同量子随机数发生器方案的量子熵源工作原理及补充测试项目等内容提出意见和建议。本次会议形成修改意见 115 条。

2026 年 6 月至 7 月，工作组对第二次会议形成的 115 条意见进行了逐条研究和处理，重点对标准题名及英文名称、全文表述统一、规范性引用文件和参考文献、术语定义及缩略语、量子随机过程表述、量子熵源结构边界、测量结果采集模块定位、随机源序列与随机数序列区分、可测试性要求、一致性与稳定性要求、随机源序列采集检测与最小熵评估、测试接口和测试设备通用要求、健康检测/失效检测、附录中不同 QRNG 方

案的量子熵源工作原理及补充测试项目等内容进行了修改完善。对于最终随机数序列随机性检测、统一最小熵计算公式、固定测试阈值、环境适应性试验等意见，工作组结合本文件聚焦量子熵源及后处理前随机源序列的定位，以及不同技术路线实现差异，进行了部分采纳和说明，形成进一步修改稿并发送工作组成员审阅，为形成公开征求意见稿奠定基础。

2026年7月2日，国家标准计划《量子随机数发生器量子熵源测试规程》第三次起草工作组会议以线上方式召开。来自合肥国家实验室、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、武汉量子技术研究院、中国信息安全测评中心、中国标准化研究院、中国计量科学研究院、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、中国人民解放军网络空间部队信息工程大学、中移量子科技有限公司、武汉光谷信息光子创新中心有限公司、中国长城科技集团股份有限公司、中科酷原科技（武汉）有限公司、江苏省计量科学研究院等25家单位的33位专家参加会议。会议审核并确认了第二次起草工作组会议纪要，对根据第二次会议意见修改完善后的标准草案进行了审议，重点讨论了形成征求意见稿前的修改内容。会上，工作组25家单位成员单位代表所属单位投票表决，投票结果同

意对工作组讨论稿（第三稿）修改完善后，形成征求意见稿和征求意见稿编制说明，向 TC578 标委会秘书处提交。投票情况：参加投票单位 19 家（超过全体成员单位数的 3/4），同意 19 家，反对 0 家，弃权 0 家；参加投票人数 24 人，同意 24 人，反对 0 人，弃权 0 人。参与投票的成员单位和专家均同意形成征求意见稿。

（四）国家标准主要起草人及其所做的工作

本标准由合肥国家实验室作为牵头单位，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等共同负责标准起草。

主要起草人员及其工作如下表 1：

表 1 标准起草人员及主要工作

序号	姓名	单位	联系方式	主要工作
1	聂友奇	合肥国家实验室	youqinie@ustc.edu.cn	牵头开展标准预研，负责标准制定总体组织协调工作，包括制定和推进工作计划、文件收集、提出标准整体框架和主要技术内容，组织讨论并提出意见建议。
2	吴佳颖	合肥国家实验室	jywu@mail.ustc.edu.cn	参与标准预研，参与标准草案及编制说明起草，组织或参与标准关键技术验证，参与讨论并提出意见建议。
3	张军	中国科学技术大学	zhangjun@ustc.edu.cn	参与标准预研，参与标准草案及编制说明起草，组织或参与标准关键技术验证，参与讨论并提出意见建议。

序号	姓名	单位	联系方式	主要工作
4	张强	中国科学技术大学	qiangzh@ustc.edu.cn	参与标准预研，参与标准草案及编制说明起草，组织或参与标准关键技术验证，参与讨论并提出意见建议。
5	白冰	中国科学技术大学	baib@ustc.edu.cn	参与标准预研，参与标准草案及编制说明起草，组织或参与标准关键技术验证，参与讨论并提出意见建议。
6	江扬帆	济南量子技术研究院	jiangyangfan@jiqt.org	参与标准预研，提供标准制定工作指导，参与标准专业技术内容审核。
7	李明翰	国科量子通信网络有限公司	liminghan@qtict.com	参与标准预研，提供标准制定工作指导，参与标准专业技术内容审核。
8	陈华	中国科学院软件研究所	chenhua@iscas.ac.cn	参与标准预研，提供标准制定工作指导，参与标准专业技术内容审核。
9	徐兵杰	中国电子科技网络信息安全有限公司	xbjpk@163.com	参与标准预研，提供标准制定工作指导，参与标准专业技术内容审核。
10	周淳	中国人民解放军网络空间部队信息工程大学	zc@qiclab.cn	参与标准讨论，提出意见和建议。
11	赖俊森	中国信息通信研究院	laijunsen@caict.ac.cn	参与标准讨论，提出意见和建议。
12	郑明睿	济南量子技术研究院	zhengmingrui@jiqt.org	参与标准讨论，提出意见和建议。
13	王超凡	济南量子技术研究院	wangchaofan@jiqt.org	参与标准讨论，提出意见和建议。

序号	姓名	单位	联系方式	主要工作
14	刘慧	合肥国家实验室	lhui@hfnl.cn	参与标准讨论，提出意见和建议。
15	姜艳	国科量子通信网络有限公司	jiangyan@qtict.com	参与标准讨论，提出意见和建议。
16	李东东	科大国盾量子技术股份有限公司	dongdli@ustc.edu.cn	参与标准讨论，提出意见和建议。
17	黄溢智	中电信量子信息科技集团有限公司	huangyizhi@chinatelecom.cn	参与标准讨论，提出意见和建议。
18	刘婧婧	安徽问天量子科技股份有限公司	liujingjing@qasky.com	参与标准讨论，提出意见和建议。
19	李华生	上海循态量子科技有限公司	huasheng.li@xtquantech.com	参与标准讨论，提出意见和建议。
20	华昕	武汉光谷信息光子创新中心有限公司	huaxin@noeic.com	参与标准讨论，提出意见和建议。
21	韩玄	武汉量子技术研究院	hanxuan@mail.ustc.edu.cn	参与标准讨论，提出意见和建议。
22	魏瑛	中移量子科技有限公司	weiyi3@cmict.china mobile.com	参与标准讨论，提出意见和建议。
23	刘宏伟	中国信息安全测评中心	hwliu_w@163.com	参与标准讨论，提出意见和建议。
24	邓玉强	中国计量科学研究院	yqdeng@nim.ac.cn	参与标准讨论，提出意见和建议。
25	张萌	中国标准化研究院	zhangmeng@cnis.ac.cn	参与标准讨论，提出意见和建议。
26	周泓伊	中国科学院计算技术研究所	zhouhongyi@ict.ac.cn	参与标准讨论，提出意见和建议。
27	张行健	香港大学	thuxjzhang@gmail.com	参与标准讨论，提出意见和建议。

序号	姓名	单位	联系方式	主要工作
28	郭晓敏	太原理工大学	guoxiaomin@tyut.edu.cn	参与标准讨论，提出意见和建议。
29	陈超	宁波大学	chenchao2@nbu.edu.cn	参与标准讨论，提出意见和建议。
30	于春霖	中国长城科技集团股份有限公司	yuchunlin@greatwall.com.cn	参与标准讨论，提出意见和建议。
31	赵品彰	江苏省计量科学研究院	lemon_jsmi@163.com	参与标准讨论，提出意见和建议。
32	刘宁	山东省体育彩票管理中心	sdyjln@163.com	参与标准讨论，提出意见和建议。

二、国家标准编制原则、主要内容及其确定依据

（一）标准编制原则和依据

本标准文件按照 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。

（1）在国内当前的技术条件下实现标准化目标具有完全可能性。

（2）本项目的技术与主流技术发展方向相符合。

（3）当前技术条件下标准可实现。

（二）标准主要技术内容说明

本指导性技术文件聚焦于量子随机数发生器中的量子熵源部分，描述了量子熵源的结构组成及工作原理，并提供了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，旨在明确量子熵源与后处理模块的边界，规范后处理前随机源序列的采集、检测和最小熵评估，为量子随机数发生器量子熵源的设计、测试和评价提供技术依据。

量子熵源是量子随机数发生器产生随机性的核心部分，其随机性来源、结构边界、可测试性、一致性、稳定性以及随机源序列中量子随机成分的最小熵评估，直接关系到后续随机性提取参数设置和最终随机数输出质量。本文件将量子熵源划分为量子随机过程模块、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，明确后处理模块不属于量子熵源本体。在测试内容上，本文件围绕量子随机过程机理审查、可测试性确认、一致性与稳定性测试、随机源序列采集检测与最小熵评估等内容建立测试规程，并结合不同技术方案给出补充测试项目，以提升不同量子熵源方案测试结果的可比性和可追溯性。

本文件的主要技术内容包括：1) 范围；2) 规范性引用文件；3) 术语和定义；4) 量子熵源结构组成及工作原理；5) 要求，包括量子随机过程要求、可测试性要求、一致性与稳定性要求、随机源序列的采集检测与最小熵评估要求；6) 测试方法，包括测试接口、通用测试环境与准备、量子随机过程机理审查、可测试性确认、一致性与稳定性测试、随机源序列的采集检测与最小熵评估；7) 资料性附录，包括不同熵源技术方案工作原理以及不同 QRNG 方案补充测试项目。

（三）标准中主要技术内容确定的依据和过程

2017 年底，中国通信标准化协会在量子通信与信息技术特设任务组开展了《量子随机数制备和检测技术研究》研究课题，由国盾量子牵头制定了通信行业标准《基于 BB84 协议的量子

密钥分发 (QKD) 用关键器件和模块 第 3 部分: 量子随机数发生器 (QRNG)》, 为国内首个量子随机数相关通信行业标准。该标准提出了 QRNG 一般结构、功能模块、应用接口等要求, 并给出了对 QRNG 模块和接口进行测试的方法。该标准在 QRNG 方案原理部分涵盖了相位噪声、真空涨落噪声、放大自发辐射噪声以及单光子分束等四类主流 QRNG 方案, 但其测试方法主要面向 QRNG 系统总体框架, 尚未针对量子熵源本体、随机源序列采集位置、量子随机成分评估以及不同技术方案的补充测试项目给出系统化规程。因此, 本文件在既有工作的基础上, 将技术内容聚焦于量子随机数发生器中的量子熵源部分, 进一步细化量子熵源结构边界、技术要求和测试方法。

2018 年 9 月, 国际电信联盟 (ITU) 发起了量子随机数发生器方面的标准研究项目, 并于 2019 年 11 月 26 日发布了《Quantum noise random number generator architecture》(ITU-T X.1702) 标准文件。该文件主要对 QRNG 进行一般功能结构划分和定义, 但未针对不同 QRNG 技术方案中的量子熵源原理、安全性分析、量子噪声与经典噪声贡献区分、随机源序列最小熵评估等内容展开, 也未给出面向量子熵源的测试规程。因此, 有必要结合我国量子随机数发生器技术发展和测评需求, 给出适用于量子熵源的结构描述、基本要求、测试接口、测试环境、测试流程和补充测试项目。

本文件主要技术内容的确定参考了 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》、

GM/T 0103—2021《随机数发生器总体框架》、YD/T 6445—2025《量子随机数发生器技术规范》、GM/T 0005—2021《随机性检测规范》以及 NIST SP 800-90B:2018《Recommendation for the Entropy Sources Used for Random Bit Generation》等国内外相关标准化文件和技术文件。其中，术语和定义优先采用国内标准化文件已有定义；量子熵源典型技术方案分类参考 YD/T 6445—2025；最小熵、IID/Non-IID 分析等熵评估思路参考 NIST SP 800-90B；后处理后随机数序列的随机性检测可参考 GM/T 0005—2021，但不作为本文件中后处理前随机源序列最小熵评估的判定依据。

在起草过程中，工作组结合相关标准、公开技术资料 and 专家意见，明确本文件的适用对象为量子随机数发生器中的量子熵源部分，而非完整 QRNG 整机。经讨论，确定量子熵源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本体。随机源序列产生模块仅指形成后处理前随机源序列所必需的采集、转换或记录环节，可包括 ADC、TDC、比较器、计数器或事件记录单元等。作出该边界划分的主要依据是：量子熵源测试需要获取后处理前的随机源序列，并基于该序列及熵源模型评估量子随机成分的最小熵下界；若不明确随机源序列产生模块及采集位置，将难以开展可追溯的熵评估和测试结果判定。

本文件在“要求”部分确定了量子随机过程要求、可测试性要求、一致性与稳定性要求、随机源序列采集检测与最小熵

评估要求。上述内容的确定主要基于量子熵源测试的共性需求：一是确认随机性来源于明确的量子随机过程；二是确认被测熵源具备测试接口、数据获取能力和必要的参数监测/健康监测能力；三是确认关键组件、物理通道、测量结果采集链路、输出接口以及多通道结构与设计文件和熵源模型保持一致；四是基于后处理前随机源序列，对量子随机成分贡献的最小熵下界进行评估，并识别、估计和约束经典噪声及其他非理想因素对评估结果的影响。

本文件在“测试方法”部分按照要求条款逐项对应设置测试内容，确定了测试接口、通用测试环境与准备、量子随机过程机理审查、可测试性确认、一致性与稳定性测试、随机源序列采集检测与最小熵评估等内容。考虑到不同量子熵源技术路线差异较大，本文件不统一规定固定测试设备型号、统一采样数量或统一判定阈值，而要求结合熵源类型、系统架构、熵源模型、产品设计文件和测试方案确定具体测试项目、测试参数及判定依据，以保证文件具备指导性和适用性。

针对不同 QRNG 技术方案，本文件设置资料性附录，给出相位涨落、真空涨落、ASE 噪声、多光子态、电子隧穿等典型量子熵源方案的工作原理，并给出相应补充测试项目。附录内容用于支撑正文通用测试方法的实施，使测试人员能够结合具体技术路线，对光源、本振光、干涉链路、光电探测链路、模数转换链路、探测阵列、偏置条件、事件分布、经典噪声影响以及随机源序列熵评估等内容开展补充核查和测试。该安排兼

顾了正文条款的通用性和不同技术方案测试实施的差异性。

三、试验验证情况的说明

本文件为量子随机数发生器中量子熵源部分的测试规程，主要用于指导量子熵源结构边界确认、测试接口设置、量子随机过程机理审查、一致性与稳定性测试、后处理前随机源序列采集检测以及最小熵评估。工作组已围绕本文件规定的主要测试内容组织开展试验验证，相关验证数据和测试报告正在进一步整理完善。

（一）主要试验的分析

本文件试验验证选取了具有代表性的量子熵源技术方案，包括激光相位波动方案、真空态涨落方案以及放大自发辐射方案。验证内容主要围绕量子随机过程确认、关键组件和采集链路一致性、测试接口可用性、随机源序列采集、分布特性分析、经典噪声影响分析以及最小熵评估等方面开展。上述方案分别覆盖连续变量型量子熵源和事件/时间标记型量子熵源，能够对本文件通用测试方法的适用性和可操作性形成支撑。

（二）主要试验验证的分析、综述报告

从已开展的验证情况看，本文件提出的测试接口设置、通用测试环境与准备、量子随机过程机理审查、可测试性确认、一致性与稳定性测试、随机源序列采集检测与最小熵评估等测试内容，能够适用于不同类型量子熵源的测试实施。通过对激光相位波动、真空态涨落和光子到达时间等方案的验证，相关测试方法能够支持对后处理前随机源序列的获取、记录和分析，

并能够结合熵源模型对随机源序列中量子随机成分的最小熵下界进行评估。

（三）试验方案设计

试验对象为采用激光相位波动方案、真空态涨落方案和放大自发辐射方案的量子随机数发生器量子熵源或相关实验系统。试验过程中，依据本文件规定的测试流程，分别开展测试接口确认、测试环境与设备记录、量子随机过程机理审查、关键参数和采集链路一致性核查、随机源序列采集、分布特性分析以及最小熵评估等工作。具体试验条件、测试数据、计算过程和结果见后续补充的试验验证报告。

（四）试验结果

基于目前已开展的试验验证工作，可以初步说明：本文件规定的量子熵源测试规程能够在现有实验条件和产品测试条件下实施，相关测试方法对不同技术路线的量子熵源具有一定适用性，能够为量子熵源测试接口确认、随机源序列采集检测、量子随机成分分析和最小熵评估提供技术依据。工作组将在征求意见阶段结合反馈意见和试验验证报告，进一步完善试验验证情况说明。

四、与国际、国外同类标准技术内容的对比情况

经调研，与本文件技术内容相关的国际、国外标准化文件主要包括 ITU-T X.1702《Quantum noise random number generator architecture》、ISO/IEC 18031:2025《Information technology — Security techniques — Random bit generation》以及 NIST SP

800-90B 《Recommendation for the Entropy Sources Used for Random Bit Generation》等。上述文件分别从量子噪声随机数发生器架构、随机比特发生器通用模型、通用熵源评估等角度给出了相关技术要求或评估思路，但尚未形成与本文件完全对应的、面向量子随机数发生器量子熵源测试规程的国际标准或国外标准。

ITU-T X.1702 主要给出了基于量子物理现象的随机数发生器功能架构，提出了量子熵源通用功能结构、熵估计和熵评估的基本思路，并说明其目的之一是区分基于量子物理的熵源与非量子物理熵源。与 ITU-T X.1702 相比，本文件在借鉴其量子熵源架构和熵评估思想的基础上，进一步结合我国量子随机数发生器产品研制和测试需求，明确了量子熵源与后处理模块的边界，规定了量子随机过程模块、测量模块、随机源序列产生模块以及参数监测/健康监测模块的结构关系，并给出了测试接口、通用测试环境与准备、量子随机过程机理审查、可测试性确认、一致性与稳定性测试、随机源序列采集检测与最小熵评估等测试规程，技术内容更侧重测试实施和结果记录。

ISO/IEC 18031:2025 主要规定了用于密码应用的随机比特发生器概念模型，以及非确定性随机比特发生器和确定性随机比特发生器主要组成要素的特性和安全要求。该文件适用于随机比特发生器总体安全框架，但不针对量子随机数发生器中的量子熵源开展专门规定，也不涉及不同量子熵源技术方案的物理机理、测试接口、随机源序列采集位置、量子噪声与经典噪

声贡献区分及最小熵评估方法。本文件则聚焦于量子随机数发生器量子熵源部分，对后处理前随机源序列的采集检测、量子随机成分最小熵下界评估以及不同技术方案补充测试项目进行了细化。

NIST SP 800-90B 主要针对随机比特发生器所使用的通用熵源，规定了熵源设计原则、要求及熵源验证测试方法，涉及健康测试、最小熵评估、IID/Non-IID 判断等内容。该文件可为本文件中最小熵概念、熵源评估和健康检测等内容提供参考，但其对象为通用随机比特发生器熵源，并未针对量子熵源的量子随机过程、量子噪声与经典噪声贡献约束、量子熵源结构边界以及典型 QRNG 技术路线给出测试规程。本文件在参考其熵评估思路的基础上，强调随机源序列中量子随机成分贡献的最小熵下界，并结合相位涨落、真空涨落、ASE 噪声、多光子态、电子隧穿等典型方案给出资料性工作原理和补充测试项目。

综上，现有国际、国外同类文件主要提供随机数发生器总体架构、通用随机比特发生器安全要求或通用熵源评估方法。本文件与上述文件在量子熵源结构、熵评估和随机源序列测试等方面具有一定衔接关系，但技术重点不同。本文件面向量子随机数发生器中的量子熵源测试，突出量子随机过程机理审查、后处理前随机源序列采集检测、量子随机成分最小熵评估、一致性与稳定性测试以及不同 QRNG 方案补充测试项目，可对现有国际、国外相关标准化文件形成补充。

五、标准采用国际文件的情况说明

无。

六、与有关的现行法律、法规和强制性国家标准的关系

经查，本标准与现有标准及制定中的标准无交叉重复，不涉及国内外专利，与有关的现行法律、法规和强制性国家标准无冲突。

七、制修订过程中是否存在重大分歧意见，以及重大分歧意见的处理过程

本标准制定过程中无重大分歧意见。

八、标准中涉及专利的情况

未发现涉及相关专利。

九、国家标准性质的建议及贯彻国家标准的要求和措施建议

鉴于本标准规定内容不涉及人身健康和生命财产安全、国家安全、生态环境安全等内容，属于基础性标准。根据标准化法及有关规定，建议本标准作为国家标准化指导性技术文件。

本标准的建议实施日期为：自发布之日起 6 个月。

本指导性技术文件的实施，为我国量子随机数发生器，特别是其中的量子熵源部分提供了测试规程，有助于明确量子熵源的结构组成、功能要求、性能检验要求等内容，对量子随机数发生器量子熵源的生产及使用提供技术指导和检测规程，促进量子随机数领域产业化应用的高质量发展。

建议保证标准文本的充足供应，使各相关方能够及时获取标准文本。对于标准使用过程中容易出现的疑问，工作组做好

必要、及时的解释工作。针对不同的使用对象，有侧重点地进行标准培训和宣贯，以保证标准的贯彻实施。

十、其他应予说明的事项

起草工作组承诺，本标准文件无版权风险。

《量子随机数发生器量子熵源测试规程》

国家标准化指导性技术文件起草工作组

2026 年 7 月 6 日